UN GUIDE COMPLET SUR

la protection contre les ransomware pour Microsoft 365

Renforcez la cyber-résilience de votre organisation

COHESITY

Sommaire

La sécurité des données compte

Le travail hybride et la réduction des coûts d'investissement constituent les principales raisons qui ont poussé les entreprises à adopter rapidement Microsoft 365. Pourtant, la suite par abonnement – y compris Exchange Online et d'autres applications de productivité d'Office 365, OneDrive, SharePoint et Teams – constitue une cible séduisante pour les cybercriminels en raison de sa large base d'utilisateurs[1] et de la croissance rapide du nombre d'abonnés[2] au cours des deux dernières années.

Si votre entreprise a recours à Microsoft 365 (M365), les procès-verbaux de collaboration et le nombre d'utilisateurs ne constituent pas les seuls éléments à surveiller. Les ransomwares se multiplient et vos données sensibles dans M365 feront de plus en plus l'objet d'attaques.

Les acteurs malveillants envisagent déjà d'infecter vos données avec des logiciels malveillants et de les chiffrer, en exigeant que votre organisation paie une rançon afin de pouvoir les récupérer. En outre, les cybercriminels espèrent que vos données sensibles ne bénéficient que d'une protection limitée dans M365 afin de pouvoir les exfiltrer, ou les voler, avant de les utiliser à des fins d'extorsion pour empêcher leur divulgation publique. Cette technique est en passe de devenir un élément des programmes de ransomware à « double extorsion ».

Quel que soit leur mode opératoire, les auteurs d'attaque par ransomware sont en mesure de porter gravement atteinte à vos résultats financiers et à la réputation de votre marque. Avoir une longueur d'avance. Les orientations de Microsoft en matière de lutte contre les ransomwares ciblant vos données M365 sont simples : Sauvegardez régulièrement le contenu et les données. Stockez en utilisant des applications et des services tiers.[3] C'est un bon conseil. Mais il en faudra probablement plus.

Continuez à lire pour découvrir pourquoi et comment améliorer votre protection contre les ransomwares pour M365 ›

66 % des entreprises ont été touchées par un ransomware

au cours de l'année écoulée.[4]

25 % déclarent que les suppressions malveillantes

constituent leur principale cause de perte de données SaaS.[5]

[1]Troisième trimestre 2022 chez Microsoft : Transcription de l'appel sur les revenus – Office 365 compte près de 300 millions d'utilisateurs
[2]Premier trimestre 2022 chez Microsoft : Transcription de l'appel sur les revenus – Plus de 50 %
[3]Contrat de service Microsoft, section 6b

[4]Sophos, « State of Ransomware 2022 », 2022.
[5]Enterprise Strategy Group. « L'évolution des stratégies du cloud pour la protection des données », 2021.

Comprendre la responsabilité partagée

En tant que fournisseur de cloud et d'applications hyperscale, Microsoft applique un modèle de responsabilité partagée. En pratique, cela signifie que Microsoft s'engage à assurer des niveaux de service élevés en matière de fiabilité et de disponibilité de l'infrastructure, une sécurité robuste de l'infrastructure et une protection des données limitée, y compris certaines stratégies de conservation des données et de gestion des versions que nous aborderons plus loin. Il ne s'engage jamais à garantir la disponibilité de votre contenu. Voilà une vue d'ensemble de sa part de responsabilité.

Votre part de responsabilité est tout aussi importante dans le maintien de la réputation de votre marque et de la confiance de vos clients. Votre contenu vous appartient. C'est donc à vous qu'il incombe de protéger vos données dans le cloud à court et à long terme, afin de répondre à vos exigences commerciales et réglementaires. Il incombe également à votre organisation de récupérer rapidement vos données en cas d'attaque. Votre part de responsabilité en interne pour M365, un environnement stratégique, constitue la raison principale d'envisager de suivre les conseils de bonnes pratiques et d'aller au-delà de la protection de base de M365 pour ajouter des applications et des services tiers qui protègent vos données contre les attaques par ransomware.

Bien que Microsoft dispose de certains moyens intégrés pour conserver les données après leur suppression ou leur modification, ces capacités ne constituent tout simplement pas des sauvegardes robustes et immuables (nous y reviendrons plus tard).

Les protections M365 natives en bref

La protection des données est importante pour les applications M365 qui servent vos opérations commerciales clés. Voici un bref aperçu de ce que Microsoft a intégré :

Exchange Online	• la rétention par défaut des éléments supprimés est de 14 jours, jusqu'à 30 jours, si configuré • la durée de conservation par défaut des e-mails supprimés est de 30 jours
OneDrive	• la conservation des éléments supprimés pendant 93 jours par défaut pour la corbeille de la collection de sites • la conservation des éléments supprimés pendant 30 jours par défaut pour la corbeille des utilisateurs • la restauration des données jusqu'à un point dans le temps pour un maximum de 30 jours, si configuré
SharePoint	• la conservation des éléments supprimés pendant 93 jours par défaut pour la corbeille de la collection de sites • la conservation des éléments supprimés pendant 30 jours par défaut pour la corbeille des utilisateurs • la conservation des sauvegardes des éléments supprimés pendant 14 jours supplémentaires • les administrateurs sont en mesure de récupérer les collections de sites et les contenus supprimés dans un délai de 90 jours
Teams	• la durée de rétention des messages varie par défaut de 1 à 7 jours • d'autres types de données ont une durée de conservation limitée en fonction des services qui les fournissent

N'oubliez pas que chaque service M365 repose également sur Microsoft Azure Active Directory. Il est donc important de prévoir un plan de sauvegarde de ce répertoire afin de pouvoir restaurer rapidement l'accès des utilisateurs finaux.

Les ransomwares sont à l'affût

Les logiciels malveillants peuvent s'infiltrer dans un système et se cacher pendant des semaines ou des mois pour se propager à d'autres systèmes avant de lancer une attaque complète. En outre, comme vous le découvrirez, le versionnage n'est pas adapté à la restauration d'un ransomware, étant donné que les restaurations doivent s'effectuer à partir d'un moment précis sur le jeu de données entier – et non sur des fichiers individuels – afin de garantir que vos données restaurées sont exemptes d'infection par le ransomware.

La menace des modèles d'affiliation de type **Ransomware-as-a-Service (RaaS)** permet aux acteurs de la menace de faire évoluer facilement leurs opérations et de cibler tout secteur ou entreprise, quelle que soit sa taille.[8]

Remarque sur les sauvegardes et le versionnage

Si vous avez besoin d'une preuve supplémentaire que M365 native n'est pas à elle seule une sauvegarde suffisamment robuste pour vos données, examinez comment elle conserve les données. Contrairement aux véritables solutions de sauvegarde, M365 utilise une technique qui s'apparente davantage au contrôle de version, c'est-à-dire à la gestion de plusieurs révisions des mêmes informations ou fichiers. En d'autres termes, le versionnage est réalisé sur la base d'un fichier individuel et chaque fichier a un historique de version différent. Le défi de cette approche réside dans le fait que les attaques par ransomware se produisent à des moments précis et ont un impact négatif sur un grand nombre de fichiers en une seule fois.

Examinons un exemple à la figure 1 de la page suivante. Une nouvelle présentation PowerPoint réalisée aujourd'hui porte la version 2, tandis qu'une feuille de calcul des prévisions de ventes vieille de plusieurs années porte la version 1278 (si tant est que tout soit configuré pour conserver autant de versions). Ce type de conservation des versions rend difficile, voire impossible, la restauration ou la récupération de milliers de fichiers à un moment donné, à travers les documents, jusqu'à la période précédant une attaque.

[8] SecureWorks. « Rapport sur l'état de la menace 2021 », 2021.

74 % d'entre eux s'appuient uniquement sur Microsoft 365

selon une enquête récente menée auprès de 381 professionnels de l'informatique, pour la restauration de données.[6]

Et,

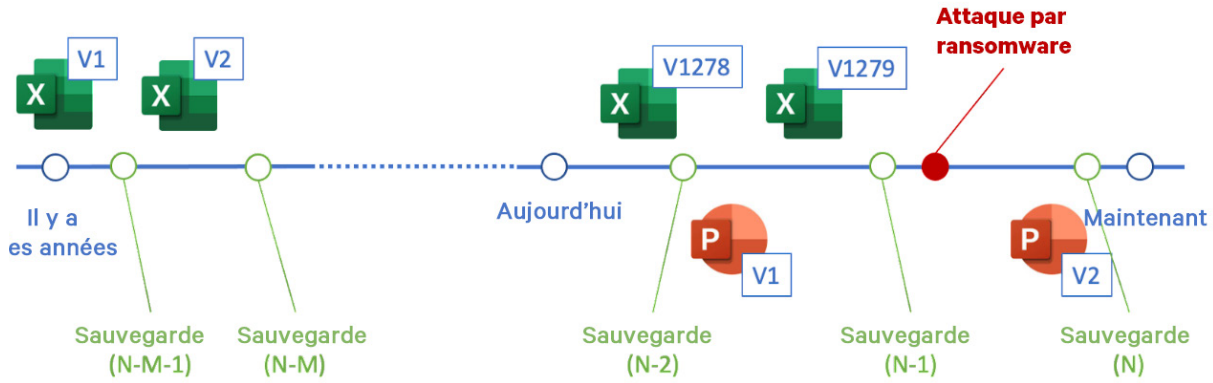
seulement 15 % des entreprises ont réussi à récupérer 100 %

de leurs données.[7]

[6] Enterprise Strategy Group. « L'évolution des stratégies de protection des données dans le Cloud – Présentation des résultats clés, » mars 2021.

[7] Enterprise Strategy Group. « L'évolution des stratégies du cloud pour la protection des données », mars 2021.

Figure 1 : Chronologie de la comparaison entre les sauvegardes et le versionnage



Une solution de gestion de données next-gen qui inclut une sauvegarde moderne permet à votre organisation de contrôler avec précision la durée de conservation des données et de restaurer toutes vos données – par snapshot – à un moment précis, par exemple juste avant une attaque ou une compromission. Ainsi, vous êtes assuré que votre équipe dispose d'une copie propre de tous vos fichiers et données à portée de main pour une restauration rapide.

Rationaliser la conformité et répondre aux demandes internes

Les réglementations gouvernementales nouvelles et évolutives ont renforcé la nécessité pour votre organisation de faire preuve de flexibilité lorsqu'il s'agit d'adapter les stratégies de conservation des données. Dans les secteurs réglementés tels que les soins de santé, les services financiers et les administrations publiques, par exemple, les équipes sont désormais régulièrement tenues de conserver les données au-delà de sept ans (et parfois même pour toujours).

Toute organisation qui a été impliquée dans un litige comprend également la valeur des stratégies de conservation flexibles. L'eDiscovery peut prendre des mois, voire des années, et implique des données M365 telles que des e-mails et des documents. Si vous ne faites pas preuve de flexibilité quant à la durée de conservation et à la rapidité de récupération de vos données, vous risquez de mettre votre organisation en situation de non-conformité ou de devoir payer des amendes pour répondre aux demandes de communication de documents.

Les dirigeants adaptent également plus souvent les orientations internes de l'entreprise aux besoins commerciaux et à la protection des données à l'ère du cloud. Ils mettent en place des stratégies qui prévoient le transfert des données hors site ou vers un autre cloud pour une protection maximale et un verrouillage minimal des fournisseurs. Vous aurez intérêt à vous assurer que vous disposez d'un plan de protection des données en cas d'interruption du service M365 ou si vous décidez un jour de passer de M365 à un autre fournisseur de cloud.

Évaluation des protections M365 actuelles

Si votre organisation a adopté la norme M365, les valeurs par défaut ont peut-être fonctionné jusqu'à présent. Considérez désormais ces questions comme un outil de décision permettant de déterminer si elles seront suffisantes à l'avenir :

- Êtes-vous protégé si le système M365 est compromis et que les seules copies de vos données sont stockées dans le cloud de Microsoft ?
- Qu'adviendrait-il de la marque et de la réputation de votre organisation si des données étaient exfiltrées et divulguées au public ou sur le dark web ?
- Comment restaurer les données nécessaires pour l'eDiscovery ou une situation juridique qui surviendrait d'ici plusieurs mois ou années ?
- Comment prendre en charge les objectifs de temps de restauration et les objectifs de points de restauration (RTO/RPO) sans que Microsoft ne propose des accords de niveau de service (SLA) ?
- Comment aborder les règles de conformité pour vos données ? Comment prouver votre conformité si vous êtes attaqué ?
- De quelles solutions de migration disposez-vous pour ramener les données sur site ou vers un autre service, si nécessaire ?
- Quelles sont vos options de sauvegarde des données M365 vers un autre cloud pour la cyber-résilience et l'isolement des données en cas d'attaque du cloud de Microsoft ?

La réponse à ces questions vous donne-t-elle à réfléchir ? Les protections par défaut de la norme M365 peuvent mettre **en danger** votre entreprise ou vos données.

Plonger dans le désastre : Comment les ransomwares provoquent le chaos

Bien que les applications disposent de capacités de conservation et de gestion des versions de base, les cybercriminels trouvent des failles. Voici des méthodes courantes utilisées pour cibler M365 à l'aide de ransomwares.

L'infection

Vous souvenez-vous de ces e-mails du prince fortuné promettant des millions de dollars en cas de réponse ? L'e-mail reste l'un des principaux vecteurs d'infection exploités par les ransomwares. Le simple fait de cliquer sur un lien ou de télécharger un document suffit à déclencher un logiciel malveillant qui chiffre les données et les systèmes des particuliers et des entreprises.

Selon le rapport 2022 State of the Phish, plus de huit organisations sur dix (83 %) ont déclaré avoir subi une attaque de phishing par e-mail réussie en 2021, contre cinq sur dix (57 %) en 2020.[9] Et rien ne laisse présager un ralentissement des menaces.

Récemment, la société d'exploitation ferroviaire Merseyrail, basée à Liverpool, a subi une attaque par ransomware Lockbit. L'attaque s'est propagée grâce à la compromission réussie d'un compte Office 365 privilégié. L'infection par e-mail, y compris par Exchange Online, constitue un vecteur courant d'accès aux systèmes d'entreprise pour les attaquants. Une fois que les acteurs malveillants ont obtenu l'accès, leur ransomware se déplace de façon latérale en utilisant des informations d'identification compromises pour attaquer en exploitant les vulnérabilités des systèmes non corrigés.

Les exemples les plus courants d'e-mails malveillants observés récemment dans les signaux de menace sont les suivants :

- **L'hameçonnage** (aussi appelé spear-phishing) : Les attaquants cherchent à inciter une personne à partager des informations sensibles en lui envoyant des notifications d'urgence l'incitant à cliquer sur un lien, par exemple afin de réinitialiser un mot de passe. Après avoir saisi leurs identifiants sur un faux domaine, les victimes sont souvent redirigées vers un site légitime, tel que la page de connexion M365, pour saisir à nouveau leurs identifiants, complétant ainsi le vol et l'escroquerie.

- **La diffusion de logiciels malveillants** : Lorsqu'un message compromis est reçu et ouvert, il peut être lié à un site web malveillant qui diffuse le logiciel malveillant sur un ordinateur professionnel. Un document infecté peut également contenir des macros qui téléchargent des ransomwares en arrière-plan, transformant ainsi les systèmes en armes permettant d'attaquer d'autres systèmes dans l'environnement.

> Le Cerber ransomware constitue un exemple notable d'attaquants se concentrant sur les utilisateurs Microsoft (Office) 365 pour diffuser des e-mails d'hameçonnage.[10]

[9] VentureBeat. « 22 très mauvaises statistiques sur la croissance de l'hameçonnage et des ransomwares, » 22 février 2022.

[10] AFI. « Un ransomware peut-il s'attaquer à vos données Microsoft 365 ? » 22 janvier 2022.

Malgré toutes les mesures de protection de base de M365, notamment la configuration correcte des règles de flux d'e-mails pour la détection du spam SCL, l'anti-spam, l'anti-hameçonnage, les liens sûrs, les pièces jointes sûres, l'authentification multifactorielle et les paramètres anti-malware, certains e-mails provenant d'acteurs malveillants parviennent toujours dans les boîtes aux lettres des entreprises. Le défi se pose avec encore plus d'acuité avec les fichiers OneDrive et SharePoint, qui présentent un risque de chiffrement plus élevé.

Lorsque les attaquants frappent, vous voulez être sûr de pouvoir récupérer rapidement, conformément aux SLA de l'entreprise. Si votre entreprise s'attend à un SLA de restauration (RTO et RPO) et à un format de restauration préféré en cas de perturbation inattendue, telle qu'une attaque par ransomware, vous aurez besoin d'une solution de protection des données pour vous aligner sur les besoins de l'entreprise et garantir la capacité de restauration. Cela signifie que la protection des sauvegardes pour l'ensemble de votre suite M365, notamment les e-mails Exchange Online, doit faire partie de votre plan informatique.

Chiffrement des données

Depuis des années, le chiffrement des données reste la stratégie privilégiée des auteurs d'attaques par ransomware. Les cybercriminels verrouillent les données de production et exigent un paiement important avant de promettre de communiquer aux équipes une clé de chiffrement (ou souvent, un ensemble de clés à fouiller) qui leur permettra de déchiffrer et de débloquer leurs données. Par exemple, OneDrive et SharePoint se trouvent déjà entre les mains d'acteurs malveillants. Ces ressources peuvent être chiffrées de plusieurs manières. Par exemple, les fichiers locaux infectés sont synchronisés à partir d'une machine utilisateur vers OneDrive ou SharePoint, ou directement à partir d'un serveur qui chiffre et synchronise les fichiers de manière évolutive. Même si vous pouviez récupérer vos fichiers grâce à l'archivage des versions, le processus reste fastidieux et ne permet pas d'effectuer une restauration ponctuelle, ce qui constitue souvent une exigence stratégique. Dans tous les cas, un système de sauvegarde et restauration immuable constitue une contre-mesure efficace.

Vol et exfiltration de données

Ce succès inimaginable a enhardi les auteurs d'attaques par ransomware, qui sont devenus plus créatifs. Les cybercriminels ne se contentent plus de chiffrer les fichiers et les données, ils les volent également. Ils suppriment de manière illégale de grands volumes de données (exfiltration) et ciblent les informations sensibles et confidentielles, notamment les numéros de carte de crédit des clients et les informations personnellement identifiables (PII), dans le but de menacer de les divulguer publiquement ou de les vendre sur le dark web afin d'extorquer des sommes encore plus importantes aux organisations victimes.

La menace de double extorsion par ransomware est idéale pour les données M365 et terrifiante pour les entreprises. M365 et d'autres applications SaaS offrant un accès en ligne facile et des contrôles de partage simples, les cybercriminels ont de grandes possibilités, mais beaucoup moins d'obstacles. Afin de les combattre, les organisations doivent surveiller de manière proactive les applications et les utilisateurs accédant aux données afin de détecter les comportements indiquant des actions cybercriminelles.

D'ici 2025, on s'attend à des paiements de 1 750 milliards de dollars

pour les ransomwares.[11]

Plus de 83 % des attaques concernent le vol de données d'entreprise

et le chiffrement de fichiers.[12]

[11] Cybersecurity Ventures. « Rapport du CISO : L'activité des ransomwares est en plein essor », 10 déc. 2021.

[12] Coveware. « Les auteurs d'attaques par ransomware passeront à la « chasse au gibier moyen » au troisième trimestre 2021 », 21 oct. 2021.

Des mesures concrètes permettant de contrôler les données et de réduire les risques

Les protections intégrées de M365 ne remplacent pas la sauvegarde moderne des données. Elles ne fournissent pas non plus une approche multicouche de la protection contre les ransomwares de M365. Soyez mieux préparé à contrer les attaques par ransomware grâce à une solution de gestion des données next-gen qui vous permet d'effectuer trois étapes clés pour défendre correctement vos données.

1. Adoptez une protection et une restauration rapides et flexibles

Que votre organisation ait besoin de se remettre d'une attaque par ransomware ou de retrouver des fichiers archivés depuis des années (bien au-delà des périodes de conservation standard de M365), vous avez besoin d'une solution de sauvegarde moderne capable de récupérer les données à tout moment, et rapidement. Grâce à une solution de sauvegarde en tant que service (BaaS) de gestion des données next-gen, vous bénéficiez de sauvegardes automatisées, de restaurations complètes et granulaires, d'un accès à la demande et d'une facilité d'utilisation.

Reprise rapide

La bonne solution BaaS peut récupérer rapidement des centaines, voire des milliers, d'e-mails ou de fichiers en cas d'attaque à grande échelle, de catastrophe naturelle ou d'erreur humaine. La restauration à grande échelle ne doit pas non plus se limiter à M365, mais vous permettre de restaurer rapidement des centaines de VM, de grandes bases de données ou de gros volumes de données non structurées à n'importe quel moment et à n'importe quel endroit.

Restauration à n'importe quel point dans le temps

Dans M365, un employé peut faire apparaître une version différente d'un même document ou d'une même présentation afin de la récupérer rapidement. Pourtant, avec le versionnage dans M365, votre organisation ne peut pas choisir un moment précis dans le temps pour obtenir un snapshot de la dernière copie propre de toutes vos données avant qu'elles ne soient compromises. C'est ce que prévoit une solution de sauvegarde next-gen. Grâce à la BaaS, vous pouvez récupérer rapidement et facilement de grands volumes de données de manière évolutive après une attaque ou une perturbation, ce qui vous permet de respecter vos RTO et RPO.

Une restauration propre là où vous en avez besoin

Pour avoir confiance dans une restauration complète, un moteur de machine learning intégré dans une solution BaaS moderne peut recommander la dernière copie propre connue. Ainsi, lorsque vous effectuez une restauration, vous avez l'assurance que les données du snapshot sont exemptes d'anomalies et de ransomware. Assurez-vous que votre solution vous permet également de récupérer les données directement à l'emplacement d'origine ou à un nouvel emplacement en cas de panne du service M365 ou si vos comptes ont été compromis.

2. Sauvegardes sécurisées

À présent que les cybercriminels ont compris que les répertoires de conservation des données et les sauvegardes fonctionnent comme des polices d'assurance, il incombe à votre organisation de redoubler d'efforts pour garantir la protection de vos précieuses données de sauvegarde. Afin d'obtenir les meilleurs résultats, choisissez une offre BaaS dotée de contrôles de sécurité rigoureux. En outre, pensez à la BaaS, où les données sont conservées dans un service de cloud séparé, en dehors de Microsoft, et qui ne prélève pas de frais supplémentaires pour la sortie des données. Si vous le souhaitez, vous pouvez donc l'utiliser pour créer une forme de séparation des données tout en éliminant le risque d'être lié à un seul fournisseur.

Snapshots immuables

Pour les cybercriminels, cibler les données de production reste un objectif prioritaire. Mais le plus souvent, ils tentent également de chiffrer ou de supprimer les sauvegardes afin de neutraliser toute possibilité de récupérer rapidement vos données de production après une attaque. Une solution BaaS next-gen dotée d'une fonctionnalité d'immuabilité permet d'éviter ces deux scénarios, étant donné que les données se trouvent dans un snapshot immuable qui ne peut être modifié, changé ou manipulé de manière accidentelle ou malveillante.

Disques non réinscriptibles (WORM)

Les WORM permettent à votre équipe de sécurité de créer et d'appliquer un verrouillage limité dans le temps sur les données grâce à des stratégies, puis de les affecter à certaines tâches pour renforcer l'immuabilité des données protégées. Comme il s'agit d'une protection que ni les responsables ni les administrateurs de la sécurité ne peuvent modifier ou supprimer, vous n'avez pas à vous préoccuper autant d'éventuelles menaces internes. Il s'agit d'une capacité de gestion des données next-gen que M365 ne fournit pas en natif.

Chiffrement des données

Recherchez une solution conforme à la norme FIPS 140-2, la norme du gouvernement américain pour les modules cryptographiques. Elle fournit l'assurance que la conception du module et la mise en œuvre des algorithmes cryptographiques sont sûres et correctes. Le chiffrement validé par la FIPS dans les BaaS modernes est apprécié au niveau mondial en tant que meilleur moyen de protection des données en vol et au repos.

Séparer les données de sauvegarde de la production

Le stockage de vos données de sauvegarde en dehors du cloud Microsoft peut contribuer à une forme de séparation des données « hors site » tout en aidant à contrecarrer les paiements de ransomware. La BaaS vous aide à équilibrer vos exigences RTO/RPO grâce à des contrôles de sécurité appropriés en stockant les données de sauvegarde dans le cloud ou à un autre endroit. Vos données de sauvegarde resteront disponibles en cas de panne de M365 et résisteront aux manipulations des cybercriminels, étant donné qu'elles sont stockées dans un snapshot immuable.

3. Respecter les SLA et simplifier les opérations de cloud hybride

En plus de renforcer la protection des données, la BaaS comprend un ensemble complet de fonctionnalités de niveau entreprise qui vous permet de décider quand, où et combien de temps conserver les informations importantes. Votre organisation dispose ainsi du plus grand choix et de la plus grande flexibilité pour protéger ses données et répondre aux exigences commerciales d'aujourd'hui et de demain.

Rétention flexible

Lorsqu'il s'agit de répondre à des exigences de conformité complexes, rien ne vaut une sauvegarde moderne par un tiers. Elle vous donne la possibilité de contrôler la durée pendant laquelle vous devez conserver les données M365 (pendant des mois, voire des années) et gère ces stratégies pour vous. De plus, la flexibilité de la conservation à long terme – au-delà des valeurs par défaut de M365 – permet à votre organisation de récupérer les données à tout moment en cas de perturbation.

Sauvegarde unifiée (Autres sources de données M365 Plus)

Dans la mesure où vous ne souhaitez pas forcément déplacer toutes les charges de travail vers le cloud pour des raisons d'avantage commercial ou de conformité, adoptez une solution de protection des données qui vous permette de sauvegarder M365, d'autres sources de données SaaS et cloud ainsi que les charges de travail sur site telles que les VM et les bases de données.

Flexibilité des tarifs

Une stratégie de gestion des données robuste tiendra également compte de facteurs autres que les ransomwares dans les décisions relatives au choix de la solution de sauvegarde. Par exemple, il est essentiel d'aligner le budget de la sauvegarde M365 sur le mode de fonctionnement de votre organisation. Comptez-vous payer en fonction du nombre d'utilisateurs, en faisant correspondre les sauvegardes aux plans M365, ou préférerez-vous consolider les données de sauvegarde à travers une variété de sources et payer en fonction de la capacité, en obtenant une visibilité sur les coûts grâce à une facture unique mesurée à l'aide de la même métrique ? La BaaS next-gen est optimisée pour la flexibilité des prix.

Sauvegarde Microsoft 365 et liste de vérification de la protection contre les ransomwares

Capacités		Fournisseur 1	Fournisseur 2	Fournisseur 3
Adoptez une protection et une restauration rapides et flexibles	Reprise rapide	☐	☐	☐
	Restauration à n'importe quel point dans le temps	☐	☐	☐
	Une restauration propre là où vous en avez besoin	☐	☐	☐
Sauvegardes sécurisées	Snapshots immuables	☐	☐	☐
	Disques non réinscriptibles (WORM)	☐	☐	☐
	Chiffrement des données	☐	☐	☐
	Séparer les données de sauvegarde de la production	☐	☐	☐
Respecter les SLA et simplifier les opérations de cloud hybride	Rétention flexible	☐	☐	☐
	Sauvegarde unifiée (Autres sources de données M365 Plus)	☐	☐	☐
	Flexibilité des tarifs	☐	☐	☐

Cohesity améliore la protection de Microsoft 365 contre les ransomwares, et plus encore

Les cybercriminels continuent de s'attaquer aux sources de données susceptibles de générer d'importants paiements de rançon. Cohesity rend votre organisation capable de défendre toutes vos données, où qu'elles se trouvent.

Cohesity DataProtect fourni en mode As a Service fournit une sauvegarde complète en tant que service pour les services M365, notamment Exchange Online et d'autres applications de productivité Office 365, OneDrive, SharePoint et Teams, ainsi que d'autres sources de données en cloud (AWS) et sur site (telles que les VM, les fichiers et les bases de données). Grâce cette solution, votre organisation dispose d'un snapshot immuable, stocké séparément de Microsoft, qui protège vos données de sauvegarde contre toute altération ou suppression malveillante. Cohesity vous permet de récupérer rapidement en cas d'attaque par ransomware ou de panne, et vous fournit une conservation flexible des données afin que vous puissiez répondre au mieux à vos exigences commerciales et de conformité. Que vous préfériez une licence liée aux utilisateurs ou à la capacité, Cohesity BaaS vous offre la flexibilité tarifaire nécessaire pour choisir le modèle qui correspond le mieux à vos besoins.

Inscrivez-vous dès aujourd'hui et profitez d'un essai gratuit de 30 jours de DataProtect fourni en mode as a Service et commencez à sauvegarder vos données Microsoft 365 en quelques minutes.

Apprenez-en plus sur Cohesity.com/fr.

COHESITY