



EBOOK

6 RAISONS DE SAUVEGARDER MICROSOFT 365

Résumé

L'utilisation de suites de logiciels de productivité comme Microsoft 365 (anciennement Office 365) et G Suite est en constante augmentation dans tous les types d'entreprises, des PME aux grandes sociétés dirigées par les nombreux acteurs du marché (fournisseurs de services gérés, revendeurs à valeur ajoutée, etc.).

Cette tendance est particulièrement prononcée aux États-Unis. L'Europe se positionne juste derrière les États-Unis avec des taux d'adoption qui n'ont cessé de croître au cours des dernières années. Aujourd'hui, [Microsoft 365 est utilisée par 65 % des entreprises](#) contre 19 % pour G Suite (données d'étude Bitglass).

Les responsables informatiques font face à de nombreux nouveaux défis, car les données des utilisateurs ne sont plus stockées sur des postes de travail ou des serveurs sur site, mais directement dans les serveurs de ces fournisseurs au sein du Cloud.

Cependant, les données présentes dans les infrastructures externalisées ne sont pas protégées contre les risques de sécurité habituels : suppression par inadvertance, ransomware et accès malveillant.

Les entreprises ne doivent pas s'imaginer que leurs données n'ont pas besoin d'être protégées sous prétexte que leur environnement informatique a migré vers le Cloud.

Sauvegarder ou ne pas sauvegarder vos données



Microsoft 365 (Office 365). Franchement, comment ne pas aimer cette suite de logiciels ? Grâce à elle, vous pouvez vous débarrasser de vos serveurs de messagerie et de fichiers vieillissants et externaliser vos applications critiques dans un espace sécurisé et administré par l'un des plus grands noms de l'univers de l'informatique.

Force est d'admettre que Microsoft a fait un excellent travail en intégrant nombre de ses solutions phares dans une offre SaaS (Software as a Service). Cette dernière a déjà conquis **150 millions de personnes** et le nombre d'utilisateurs ne cesse d'augmenter. Vos e-mails, vos fichiers OneDrive et vos données SharePoint sont globalement en sécurité dans le Cloud.

Rappelez-vous que Microsoft 365 repose sur le transfert des applications Microsoft de base (messagerie électronique incluse) vers le Cloud. Les équipes sur le terrain doivent toujours administrer et protéger les données générées au sein de cette infrastructure cloud.

Comme Microsoft 365 vous permet de créer et de partager un très grand nombre d'informations critiques, la sécurité et la conservation des données restent des enjeux primordiaux. La plate-forme propose toujours un niveau de protection raisonnable.

Malgré cela, dans cet e-book vous découvrez les raisons pour lesquelles il est important d'envisager de déployer des outils de protection supplémentaire.

Pourquoi continuer à gérer la sécurité de vos données ?

Lorsqu'on parle de sécurité des données, il ne faut pas oublier qu'un arbre peut parfois cacher la forêt ! La société Microsoft elle-même déclare que les infrastructures à administrer sont de plus en plus hybrides et complexes. Une entreprise moyenne continue de gérer des dizaines de produits de sécurité distincts sur une myriade de systèmes¹.

Il faudra encore attendre avant d'obtenir un tableau de bord exhaustif, une infrastructure totalement invisible et une sécurité parfaitement infaillible.

Même avec tous les outils de sécurité disponibles actuellement, il est impossible de détecter toutes les menaces en temps réel. Selon le Ponemon Institute, en 2018, le [délai moyen de détection d'une perte de données était d'environ 200 jours](#)².

Devoir patienter plus [de six mois pour découvrir que des données sont potentiellement compromises](#) est particulièrement inquiétant ! Heureusement, il est possible d'agir en investissant dans des solutions tierces de protection des données qui garantissent la sécurité des actifs numériques pendant et après cette période.

De nombreuses entreprises déploient des solutions SaaS qui ne possèdent pas de plan de sauvegarde cohérent et automatisé. Ces mêmes entreprises ne sauvegardent plus leurs données et se reposent sur des fournisseurs SaaS qui ne proposent que des offres de stockage de données. Cette situation est préoccupante car, en général, un fournisseur SaaS comme Microsoft 365 fixe des limites à la quantité de données qu'il est prêt à traiter pour les entreprises.

Le prestataire SaaS fournit infrastructure, redondance, disponibilité et failover (basculement automatique vers un système alternatif), mais [il propose rarement une gestion des versions de données à long terme et une capacité de stockage généreuse, voire illimitée](#).

Et lorsque ces options sont disponibles, les coûts associés sont souvent si élevés qu'ils ne sont définitivement pas viables.

//

Le Ponemon Institute a calculé qu'en 2018, le délai moyen de détection d'une perte de données était d'environ 200 jours²

Larry Ponemon, président et fondateur du Ponemon Institute

¹ Source : [6 steps to holistic security \(Microsoft\)](#)

² Source : [Cost of a Data Breach, Ponemon, 2018](#)

En d'autres termes, **les solutions SaaS ne constituent pas une véritable alternative pour le stockage et la sauvegarde des données de votre entreprise.**

En outre, tous les fournisseurs SaaS, même Microsoft 365, peuvent voir leur système tomber en panne, perdre des données, faire faillite, modifier leur niveau de service ou être eux-mêmes victimes de la cybercriminalité. Grâce aux solutions hybrides et aux offres complètes de sauvegarde et de restauration, vous restez maître de vos données en

toutes circonstances. Pour employer une expression un peu galvaudée : il ne faut pas garder tous ses œufs dans le même panier.

Les 6 raisons suivantes devraient vous convaincre de compléter votre installation Microsoft 365 avec une véritable solution de sauvegarde et de récupération de données.



RAISON N°1

Les risques externes

Si les responsables informatiques et leurs équipes sont chargés de gérer les risques internes, il existe néanmoins certaines menaces et situations qui échappent à leur contrôle. Notamment tous les problèmes relatifs au service SaaS, qui vont de **la restriction de service partielle à la cessation complète des activités**, avec ou sans préavis.

La restriction de service partielle est un incident à court terme fréquent qui consiste à limiter l'accès à certaines données pour une courte durée. Cela est parfois dû à un problème de réseau interne, à une perte de serveurs ou de nœuds de stockage chez le fournisseur, et le processus de récupération s'enclenche : de nouveaux serveurs sont automatiquement attribués et lancés, le système d'exploitation et les logiciels appropriés sont alors chargés sur ces mêmes serveurs.

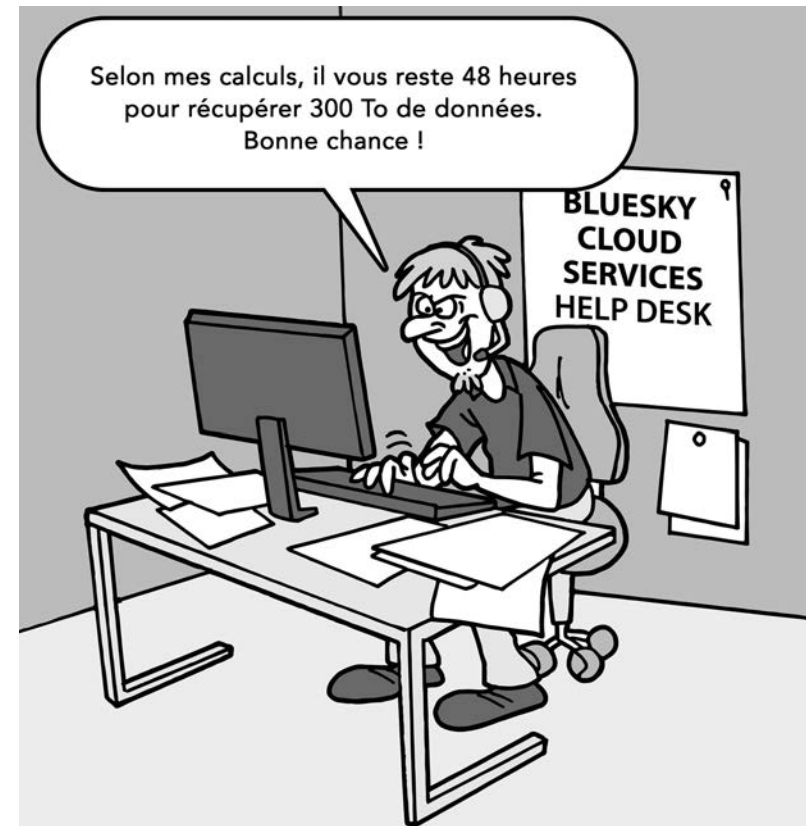
Les données sont automatiquement clonées par les processus internes de récupération de service (un Cloud intelligent semblable à un processus RAID). Cela semble convenable. La plupart du temps, vous ne le remarquerez même pas. Mais vous constaterez parfois que la dernière version des données d'un dossier spécifique a un mois.

Ces pertes de données sont parfois insignifiantes, mais il est également possible qu'elles entraînent des répercussions critiques.

Vous aurez également sans doute entendu parler de cette malheureuse histoire de plate-forme SaaS qui décide de fermer tous ses services avec un préavis de deux semaines. Elle exige ensuite de ses clients qu'ils récupèrent leurs données avant la fin du délai sous réserve de tout perdre. Malheureusement, récupérer d'importants volumes de données en peu de temps fonctionne rarement bien, sans compter le fait que tous les clients s'appliqueront à le faire dans la même période.

Ce type de situation a déjà fait perdre des données à de nombreuses entreprises. Bien sûr, c'était le début des services SaaS. Si une telle situation devait se produire aujourd'hui, le fournisseur proposerait certainement un délai plus long à ses clients. Toutefois, il est peu probable que cela suffise à empêcher certaines pertes de données, car **nous stockons désormais dans le Cloud de bien plus importants volumes de données critiques.**

En conclusion, si vous estimez que vos données stockées dans le Cloud ont une valeur significative pour votre entreprise, vous devriez vous poser la question suivante : « **Pouvons-nous continuer de travailler sans une partie des données sauvegardées dans Microsoft 365 et Exchange ?** »



RAISON N°2

Les risques internes

Le groupe Aberdeen a récemment indiqué que **32 % des entreprises avaient déjà perdu des données sauvegardées dans le Cloud³**. La plupart de ces pertes sont dues à des erreurs humaines, comme le fait de se reposer sur la corbeille de recyclage et les dossiers de courriers supprimés pour espérer récupérer ses données, et constater ensuite que les données n'existent plus ou que la seule version restante est une mauvaise version.



Certaines pertes de données surviennent également lors d'un changement de fournisseur SaaS ; **les données stockées sur l'ancienne plate-forme sont souvent supprimées définitivement après 30 jours**. Une équipe de transition pourrait facilement ne pas trouver le temps de transférer les données sauvegardées chez le précédent fournisseur parce qu'elle est trop occupée à préparer l'installation chez le nouveau. En outre, la migration des données des abonnements SaaS est souvent manuelle et complexe, elle est donc parfois négligée ou effectuée partiellement.

Malheureusement, des actes malveillants d'employés mécontents, actuels ou anciens, continuent d'être à l'origine de la suppression de courriers électroniques et de fichiers. Toute personne ayant accès au compte d'administration Microsoft 365 d'une société peut rapidement faire beaucoup de dégâts. Bien que Microsoft 365 propose une option pour empêcher toute modification de la période de conservation des données vers une durée plus courte, personne ne sait combien d'entreprises ont choisi cette option. Si votre société est l'une d'entre elles, **vous devrez tout de même faire en sorte que les plus longues périodes de conservation soient supérieures à 200 jours pour considérer vos données protégées.²** Comme nous l'avons vu dans la section précédente, rappelez-vous qu'il s'agit du délai moyen requis **pour détecter une perte de données**.

Il est fortement recommandé de créer des copies de sauvegarde et d'en soumettre la gestion à un autre administrateur afin de réduire le risque d'une perte définitive d'importants volumes de données.

Certaines solutions permettent d'archiver les courriers électroniques. **L'archivage est une fonction utile, mais** il ne doit pas se substituer à une véritable sauvegarde. En effet, l'archivage supprime les données primaires et les transfère vers un autre lieu, généralement unique. **La meilleure pratique en matière de sauvegarde de données consiste à disposer de plusieurs copies ou versions d'un ensemble de données** sur au moins deux sites physiques et sur des supports distincts.

³ Source : *Solutions review*

RAISON N°3

Les stratégies de rétention

Microsoft 365 possède une stratégie limitée en matière de conservation des objets supprimés. Par exemple, le délai maximal de rétention des dossiers vides est de 30 jours.

Les concepts de versions de sauvegarde, d'objets manquants et de conservation à long terme n'existent pas. En cas d'intrusion ou de perte de données, **5 mois entiers peuvent s'écouler après la suppression définitive de vos données par Microsoft 365.**

Il est recommandé de conserver plusieurs versions d'une partie ou de l'intégralité des contenus des messageries dans les locaux, dans une autre plate-forme Cloud ou sur bande.

Les restaurations rapides et granulaires peuvent prendre beaucoup de temps à partir de Microsoft 365, car l'application sert à gérer les e-mails et non les sauvegardes. **Vous ne pouvez pas, par exemple, remonter dans le temps** pour voir à quoi ressemblaient les e-mails et les dossiers à un moment donné ou sélectionner des objets à restaurer en fonction de recherches par mots clés ou par dates de création.

Assurez-vous que vous disposez des outils nécessaires pour assurer une certaine souplesse au niveau de votre processus de récupération des e-mails. Dans l'idéal, **il devrait inclure des sauvegardes à court terme et des sauvegardes à long terme, ainsi qu'une procédure d'archivage.**

Il faudrait également disposer d'une gamme d'options plus granulaires pour la récupération des e-mails et des dossiers et d'un système de restauration complète des messageries ou de la base de données.

Puisque **les courriers électroniques contiennent encore des données uniques critiques**, notamment dans leurs pièces jointes, la solution de récupération doit être rapide.

Si vous pouvez récupérer les messages directement depuis Microsoft 365, c'est formidable. Mais si le service est en panne ou si vous avez besoin de données plus anciennes, vous devrez alors faire appel à un véritable outil de sauvegarde et de récupération de données.



RAISON N°4

Les réglementations

En matière de contrat Saas, la confiance est primordiale. Le client d'un fournisseur SaaS lui remet également les données confidentielles de sa clientèle. Le fournisseur étant seul responsable de l'infrastructure cloud, il peut exister un conflit entre le service qu'il propose et la réglementation du pays ou de la région dans lesquels les données sont créées et administrées.

En tant qu'entreprise et client SaaS, vous gardez le contrôle sur les services que vous utilisez et les données que vous collectez. Il est impératif de connaître les réglementations sur la protection des données personnelles dans leur intégralité afin de s'assurer que toutes les informations collectées auprès de vos clients restent protégées.

Le RGPD peut être à l'origine de situations potentiellement conflictuelles relatives aux données privées et à leur conservation sur une plate-forme cloud. Il est peu probable que cette législation soit assouplie dans les années à venir. Au contraire, certains fournisseurs de SaaS seront de plus en plus en désaccord avec les lois internationales sur les données informatiques.

D'un point de vue commercial, mais aussi réglementaire, quel que soit le lieu où siège votre entreprise, **il est désormais obligatoire de protéger ces données** qui sont devenues des ressources centrales pour votre société. **Les données sont essentielles à la continuité de vos activités.**

Selon votre localisation, vous êtes également soumis à des obligations liées à la procédure e-discovery ou à des réglementations similaires en matière de recherche et de conservation d'e-mails et des données de procès ou de litige.

Ces **réglementations exigent que vous exerciez un contrôle rigoureux de vos données, car votre PDG est légalement responsable de** la mise en œuvre des outils qui conservent et stockent ces données durant la période requise. Ici encore, les mots clés sont « vos données ». Un logiciel SaaS n'est rien d'autre qu'un produit dont l'intérêt pour la conservation réglementaire et à long terme des données numérique est limité.



RAISON N°5

Les stratégies de sauvegarde 3-2-1

Le photographe américain [Peter Krogh](#) a écrit qu'il existait deux types de personnes : celles qui ont connu un problème de stockage entraînant une perte de données et celles qui en souffriront un jour. Partant de ce constat, [il a développé une approche 3-2-1 pour le stockage des données](#) qui consiste à sauvegarder les données primaires sur deux autres supports au minimum, idéalement en deux lieux différents.

En ce qui concerne Microsoft 365, les données primaires sont dans le Cloud avec Microsoft. D'autres copies peuvent être placées sur un disque dur ou sur bande en dehors du site et dans un autre lieu que le Cloud.

Le risque de perte totale des données est ainsi réduit de manière exponentielle grâce à la diversification des supports et des lieux de stockage.

Puisque [nous vivons bel et bien à l'ère de la cybercriminalité](#), prenons l'exemple de ransomwares (logiciels de rançon) où des fichiers chiffrés se propagent à travers des données primaires vers des données secondaires et des copies de sauvegarde. [Les fichiers infectés peuvent voyager sur le réseau et contaminer d'autres stockages](#) ; une simple pièce jointe ouverte dans un e-mail peut éteindre un ou plusieurs terminaux, et même infiltrer des données sauvegardées

Une solution consiste à disposer d'une destination de stockage de secours de type « air gap ». Le stockage « air gap » rassemble tout ce qui n'est pas accessible sur un réseau et qui est généralement sauvegardé sur bande hors ligne ou sur un disque optique à haute densité. Utilisé et utile pour l'archivage et les sauvegardes à long terme, les données [stockées de cette](#)



[de cette manière peuvent permettre à de nombreux administrateurs de se sortir de situations délicates dans lesquelles ils doivent faire face à une cyberattaque massive contre des systèmes et des données critiques.](#)

Plus le volume de données hors ligne est important, plus la restauration peut prendre du temps. L'[avantage d'une approche 3-2-1](#) réside dans votre capacité à restaurer rapidement les données en cas d'incident mineur ou d'incident de routine et votre capacité à restaurer les données en cas de perte catastrophique sur les stockages primaires et secondaires.

RAISON N°6

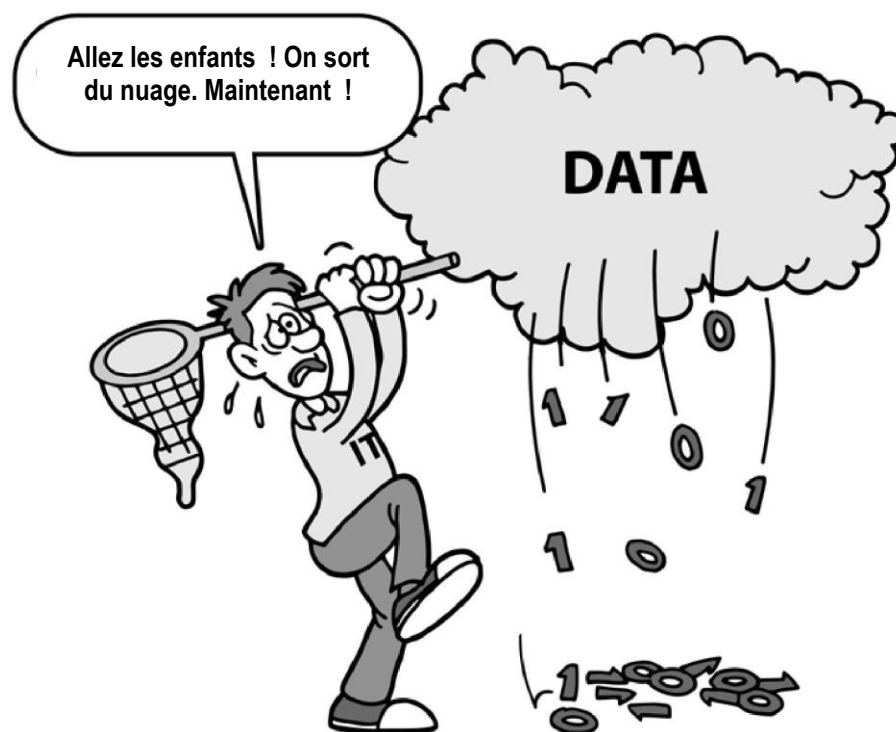
Sortir de l'environnement SaaS

Si vous faites partie du secteur depuis plusieurs années, vous savez que la gestion des infrastructures informatiques est une question de cycles. Si le cycle actuel repose sur l'externalisation, le stockage, le transfert de « charge » vers des services spécialisés, l'objectif n'est pas seulement de réduire les coûts d'infrastructure.

On observe **une forte tendance à étendre le système informatique des entreprises au Cloud** afin de faciliter l'ajout et la suppression à la demande des serveurs, des services et des utilisateurs.

Les enjeux actuels sont entièrement tournés vers la rentabilité. Cette situation offre de nombreuses possibilités pour optimiser les infrastructures, tirer parti de services spécialisés et étendre rapidement la portée d'une entreprise en fonction des besoins de ses activités.

Cette course à la productivité ne doit cependant pas nous pousser à agir **aveuglément** : l'ensemble des applications et des services critiques doivent être réversibles. Il est impératif d'étudier une option alternative à l'hébergement SaaS afin de garantir une capacité de réversibilité continue. En ce qui concerne Microsoft 365 et les e-mails, nous recommandons le déploiement d'une infrastructure mixte SaaS/sur site.



Disposer d'une solution de sauvegarde du courrier électronique qui couvre à la fois les serveurs de messagerie sur site et dans le Cloud est un outil évident qui facilite le changement lorsque celui-ci s'avère nécessaire.

Tant que vous y êtes... ne vous arrêtez pas là : votre capacité de sauvegarde et de restauration doit renforcer les applications et les bases de données pour simplifier la tâche de votre équipe de gestion informatique.

CONCLUSION

Il est clair que, dans de nombreux domaines, y compris les SaaS, que les infrastructures hybrides sont la voie à suivre... Quels que soient vos besoins, le Cloud offre flexibilité et redondance hors site tout en permettant de gérer les pics d'activité. Le concept « sur site » signifie que vous avez le contrôle de vos données localement, la possibilité de redémarrer les applications critiques de l'entreprise, y compris le courrier électronique, si des données sont perdues à cause d'une panne du Cloud ou d'une erreur humaine.

Nous ne souhaitons pas le retour des serveurs sur site, des frais de maintenance et des interruptions d'activité associées à cette architecture. Nous pensons que les SaaS peuvent parfois nous faire perdre de vue nos données réelles et qu'en cas d'incident majeur à venir, savoir ses données disponibles et sous contrôle est un sentiment particulièrement réconfortant.

Chez Atempo, nous **cherchons toujours les avantages concrets des révolutions** technologiques actuelles qui peuvent bénéficier à nos clients. Microsoft 365 est le fer de lance de la gestion des données commerciales critiques. Les solutions Atempo permettent de s'assurer que vos données continuent à évoluer dans votre écosystème.

***Pour en savoir plus sur notre solution phare,
découvrez ci-dessous
Tina et son intégration complète à Microsoft 365.***



Avantages Tina

La sécurité informatique est rapidement en train de devenir le facteur clé sur lequel reposent les achats de technologies de l'information. La vitesse, les performances et la fonctionnalité sont bien sûr essentielles, mais sans un respect fondamental de la sécurité et de l'intégrité des données, les autres avantages n'ont plus grand intérêt. Nous aimerions tous conduire une Ferrari, mais peu d'entre nous le feraient sans ceinture de sécurité ! La solution Tina offre une protection complète des courriers électroniques de Microsoft 365.



Sécurité des données et des infrastructures

La sécurité s'articule autour de trois pôles :

- **Chiffrement des données** au repos et à la volée, plus droits d'accès avancés pour empêcher la fuite et la corruption des données.
- **Partitionnement des données**. Tina sauvegarde les données dans différents lieux sécurisés, y compris des cibles « air gap » pour empêcher la propagation des cyberattaques.
- **Reporting**. Pour respecter les obligations réglementaires, Tina fournit des rapports qui vous indiquent l'endroit où se trouvent vos données, leur durée de conservation et les personnes disposant d'un accès à ces informations.

Souveraineté des données

Un nombre croissant de clients Atempo cherchent à stocker leurs données plus près de leur entreprise et à réduire la dispersion dans des stockages cloud éloignés. La souveraineté peut consister à refuser de soumettre ses données à cause du risque d'exploitation par une puissance étrangère, même si cela est légal. Il peut aussi simplement s'agir de reprendre le contrôle de vos données en ces temps de forte réglementation et de risques élevés.

Tina assure la protection des solutions SaaS sur site et hors site. Vous pouvez décider de restreindre les données stockées dans le Cloud pour éviter les problèmes de sécurité et de souveraineté et vous aligner sur la réglementation de votre pays.

Protection globale, Récupération granulaire

Il n'est pas rare que les entreprises gèrent plusieurs solutions de sauvegarde pour leurs systèmes, applications et fichiers. Tina est réputée pour son approche complète et ses solutions globales pour toutes les machines virtuelles et physiques, le multi-OS et la sauvegarde à chaud des applications et des bases de données avec récupération granulaire.

Cela signifie que vous gérez moins de solutions de protection des données et qu'il vous suffit de superviser un simple tableau de bord.

En ce qui concerne Microsoft 365, Tina vous permet de rechercher les e-mails et les boîtes de réception manquantes, mais aussi de « remonter dans le temps » pour trouver les données à récupérer. La récupération est rapide, simple et granulaire.

Rentabilité

Tina dispose d'une source très puissante et d'un moteur de déduplication global qui permettent de réaliser des économies importantes sur le stockage de sauvegarde tout en réduisant l'impact de la sauvegarde sur votre réseau. La pièce jointe d'un e-mail envoyé à 30 utilisateurs ne sera sauvegardée qu'une seule fois.

Le modèle de licence de Tina est conçu pour vous rendre la vie aussi simple que possible. L'ajout d'une messagerie sur Microsoft 365 n'aura pas d'incidence sur votre licence et ne réduira pas le niveau de protection offert à vos équipes.

Pour plus d'informations, scannez ce code QR et venez découvrir notre solution :



À propos d'Atempo

Atempo est un éditeur de logiciels indépendant européen doté d'une présence mondiale établie qui fournit des solutions de protection, de stockage, de migration et de récupération d'ensembles de données critiques à des milliers d'entreprises dans le monde. Avec plus de 25 ans d'expérience dans le domaine de la protection de données, Atempo propose une gamme complète de solutions éprouvées pour la sauvegarde de serveurs physiques et virtuels, la protection des postes de travail et la migration de fichiers entre stockages de très grande capacité. **Les trois solutions phares d'Atempo, Lina, Miria et Tina, ont obtenu les labels « France Cybersecurity » et « Utilisé par les armées françaises ».**

Sélectionné pour rejoindre le French Tech 120, un programme gouvernemental conçu pour soutenir 25 licornes d'ici 2025, Atempo possède un siège à Paris et dispose d'une présence en Europe, aux États-Unis et en Asie avec un réseau de plus de 100 partenaires, intégrateurs et fournisseurs de services gérés.

Suivez Atempo sur les réseaux sociaux :



<https://www.linkedin.com/company/atempo/>



<https://www.facebook.com/Atempo-Data-Protection-467109966988082/>



<https://twitter.com/Atempo>



Pour plus d'informations : www.atempo.com