451 Research | PATHFINDER REPORT

Prendre le contrôle de vos données Office 365

COMMANDÉ PAR

VEEAM

MARS 2019

À propos de ce document

Les rapports Pathfinder guident les décideurs à travers les questions qui entourent une technologie ou une analyse de rentabilité. Ils explorent les avantages métier d'une adoption et préconisent des points d'attention et des étapes pratiques à suivre dans le processus de décision.

À PROPOS DE L'AUTEUR

STEVEN HILL

ANALYSTE EN CHEF, STOCKAGE

Steven Hill est analyste en chef pour les technologies de stockage. Il travaille sur la dernière génération de systèmes hyperconvergés, de stockages basés sur le cloud et de solutions de continuité et de reprise après incident destinées aux grandes entreprises.

Synthèse

Les applications modernes en mode SaaS, telles que Microsoft Office 365, peuvent offrir plusieurs avantages par rapport au modèle de consommation logicielle traditionnel pour de nombreux clients professionnels. Mais la flexibilité accrue des licences de type cloud et la disponibilité des stockages cloud partagés posent de nouveaux défis en matière d'administration des données. La disponibilité des applications dans le cloud s'avère extrêmement résiliente. Toutefois, protéger les données SaaS d'Office 365 contre des risques tels que la suppression accidentelle, les menaces de sécurité et les lacunes de la stratégie de rétention — tout en satisfaisant à des conditions de sécurité évolutives dans un contexte de conformité réglementaire — impose le besoin continu de protection et de contrôle traditionnels offerts par une sauvegarde Office 365 automatisée et vérifiable.

Les fournisseurs de SaaS mettent principalement l'accent sur la protection de leur propre infrastructure pour respecter leurs accords de niveau de services (SLA) contractuels. Mais cette protection ne s'étend pas aux données des clients créées et stockées sur ces plateformes. Compte tenu des questions de responsabilité qui peuvent en découler, c'est compréhensible. La plupart des licences SaaS comportent une clause indiquant que la protection des données reste à la charge du client et non du fournisseur. Cela pose une question à un million de dollars : « Que devez-vous faire pour protéger et contrôler vos données Office 365 ? »

Principales conclusions

- **Les courriers électroniques et documents Office 365 partagés et stockés dans SharePoint, OneDrive et Teams constituent les nouvelles données stratégiques.** De nombreux plans de continuité/reprise de l'activité (BC/DR) commencent par la protection des principales bases de données et d'autres applications stratégiques. Mais les données non structurées générées par les produits SaaS commencent à croître plus rapidement que les informations des bases de données traditionnelles, et leur perte ou leur destruction peuvent avoir des conséquences tout aussi dramatiques.
- **On pense souvent à tort que les données SaaS sont protégées par nature.** Le cloud public s'avère extrêmement fiable et bien que les plateformes SaaS elles-mêmes soient protégées contre les interruptions de service de manière interne, la responsabilité du client est de sécuriser, de protéger et de concevoir des règles de rétention pour ces données situées dans le cloud.
- **Les options étendues de restauration et de gouvernance deviennent presque aussi importantes que la sauvegarde des données elle-même.** Une grande partie de la proposition de valeur d'une plateforme de sauvegarde pour les données de type Office réside dans la flexibilité de ses capacités de restauration et d'administration. Alors que le stockage SharePoint et OneDrive d'Office 365 offre des outils d'archivage des données et de conception de workflows, ce n'est pas pas le substitut d'une sauvegarde Office 365, dans laquelle toutes les données sont indépendantes de la plateforme cloud elle-même et administrées au moyen d'un ensemble d'outils qui offrent une restauration plus granulaire, plus de sécurité et une gouvernance améliorée.

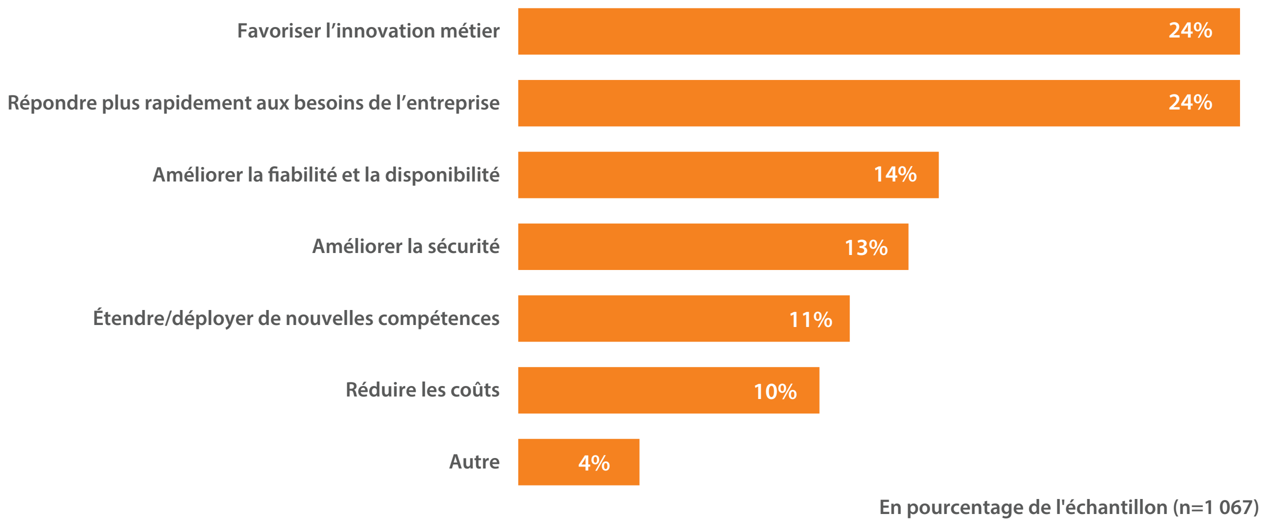
- **La protection des données sera de plus en plus régie par de nouvelles contraintes légales et de conformité.** La sauvegarde traditionnelle des données donne une priorité spécifique à la prévention des pertes de données. Mais les législations relatives à l'e-discovery et à la protection de la vie privée, telles que le Règlement général sur la protection des données (RGPD) de l'UE et le récent California Consumer Privacy Act de 2018, définissent de nouvelles règles fondamentales en matière de protection et de gouvernance des données. Maintenir une sauvegarde Office 365 peut répondre à une grande partie des conditions essentielles de protection et de sécurité des données. Cela peut aussi servir de jeu de données de référence à analyser pour satisfaire aux règles de conformité qui exigent que les entreprises soient en mesure de localiser, divulguer et même offrir à la demande une suppression vérifiable de toute donnée contenant des informations personnellement identifiables.

L'évolution de l'informatique d'entreprise et le nouveau rôle des données SaaS

Dans l'environnement métier actuel piloté par l'IT, la vitesse est essentielle. C'est le cas depuis des décennies et l'adoption de la technologie appropriée s'avère être un facteur essentiel de réussite et de croissance des entreprises dans pratiquement chaque segment vertical du marché. Aujourd'hui, le modèle de fourniture par le cloud offre aux entreprises une nouvelle manière flexible de consommer les applications, les infrastructures, les services et les données. Mais le véritable défi de l'IT consiste encore à trouver la juste combinaison de technologies pour atteindre les objectifs métier. Pour cerner ce à quoi ressemblent ces objectifs au niveau de l'ensemble du marché, nous demandons régulièrement au personnel IT de plus de 1 000 grandes entreprises — par l'intermédiaire du service 451 Research Voice of the Enterprise (VotE) — d'évaluer les aspects les plus importants de leur environnement (figure 1) et nous constatons régulièrement que l'innovation et la réactivité arrivent en tête des priorités.

Figure 1 : Objectifs les plus importants de l'informatique d'entreprise au cours de l'année suivante

Source : 451 Research Voice of the Enterprise : Digital Pulse, Vendor Evaluations 2018
Q : Quel est l'objectif le plus important de l'informatique dans votre entreprise au cours des 12 prochains mois ?



Le logiciel à la demande est l'une des principales technologies issues du cloud contribuant à faire progresser l'innovation et la réactivité. Le modèle SaaS offre des caractéristiques clés, telles que des licences flexibles et la cohérence des versions qui peuvent favoriser la productivité et l'interactivité des utilisateurs finaux. Pour l'entreprise, il est difficile de nier la commodité du modèle SaaS. En particulier dans le cas de suites d'applications telles qu'Office 365, qui ajoute des capacités de collaboration cloud à la création et à l'administration de documents, d'e-mails et d'autres contenus stratégiques.

De plus, Office 365 offre des options intégrées de stockage dans le cloud public avec SharePoint, OneDrive et Teams. Ces options peuvent réduire le besoin de stockage local et simplifier l'accès aux données partagées dans le cadre de la collaboration. Mais on pense souvent à tort que les données SaaS des clients sont sécurisées et protégées parce qu'elles se trouvent déjà « dans le cloud ». La vérité est qu'elles ne le sont pas. Et dans le cas d'Office 365, l'accord de licence stipule clairement que la protection adéquate des données reste la responsabilité du client. C'est là où l'informatique de l'entreprise doit entrer en action et aider les principales parties prenantes à déterminer des stratégies de protection, de sécurité, de disponibilité et de rétention des données appropriées, puis à trouver la combinaison optimale de technologies qui y répond. Bien que cela puisse compliquer l'adoption du SaaS au premier abord, un plan hybride et cohérent de protection des données sera très vite amorti en cas de panne des systèmes susceptible d'avoir des conséquences sur les données stratégiques ou soumises à des règles de conformité.

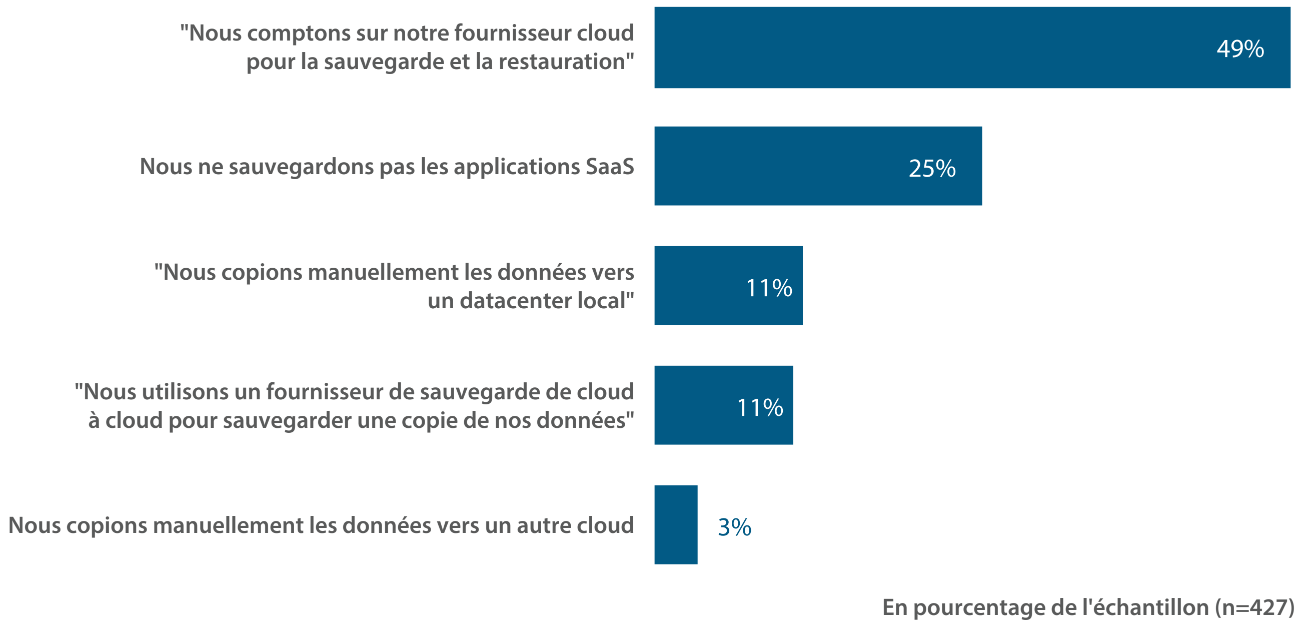
Sauvegarde de données SaaS dans le cloud public — loin des yeux, loin du cœur ?

La sauvegarde des données reste l'un des des principes fondamentaux de la protection des données pour plusieurs raisons. De plus, alors que les fournisseurs de SaaS mettent l'accent sur la résilience de l'infrastructure et la disponibilité des applications pour leur propre plateforme, la traditionnelle règle du 3-2-1 de la sauvegarde fait toujours figure de meilleure pratique pour assurer la protection et la résilience des données. Avec les données SaaS, la dynamique change parce que les données d'origine peuvent avoir été créées et exister uniquement sur la plateforme de stockage cloud du fournisseur de SaaS. Elles doivent être sauvegardées vers un second emplacement indépendant — soit sur une cible de stockage IaaS cloud distincte, soit en local si les obligations de conformité sectorielle l'exigent.

Les datacenters cloud de Tier 1 sont conçus pour fournir une disponibilité, une sécurité et une résilience 24/7/365 de tout premier ordre, mais même à ce remarquable degré d'ingénierie, la plupart des fournisseurs de cloud recommandent encore un modèle englobant plusieurs datacenters et/ou zones de disponibilité pour assurer la protection contre les pannes. Le problème est que le modèle de réplication qu'ils utilisent pour protéger leurs propres systèmes n'est pas identique à une sauvegarde indépendante de vos données SaaS. Les résultats du sondage VoTE de 451 ci-dessous illustrent les incohérences dans la manière dont les clients protègent et administrent leurs données SaaS.

Figure 2 : Protection des données SaaS

Source : 451 Research Voice of the Enterprise : Storage, Budgets and Outlook 2017
Q : Quelle est la principale stratégie de protection des applications SaaS de votre entreprise ?



Parmi les cinq options énumérées en figure 2, seuls 11 % des personnes interrogées ne sont pas loin de répondre au besoin essentiel d'une sauvegarde cohérente et automatisée. Bien qu'il n'est pas obligatoire que la sauvegarde se fasse par l'intermédiaire d'un fournisseur de sauvegarde cloud à cloud, il est indispensable qu'elle soit indépendante de la plateforme cloud elle-même**.** Une copie manuelle de n'importe quel type peut s'avérer inefficace et sujette à l'erreur, et les 25 % qui n'effectuent aucune sauvegarde jouent un jeu dangereux qui peut leur coûter cher. La part de réponses la plus importante indique faire confiance au fournisseur de cloud pour effectuer la sauvegarde et la restauration, mais cette option est viable seulement si un fournisseur SaaS offre spécifiquement des services de sauvegarde et de restauration complets. La plupart d'entre eux ne le font pas et ce malentendu soulève un risque majeur pour les données stratégiques. En définitive, les choses se résument à la règle de meilleure pratique selon laquelle les données doivent être sauvegardées vers un second système ou emplacement, qu'il soit de type cloud à cloud, ou cloud à site local.

Office 365 et l’importance croissante de ces données stratégiques

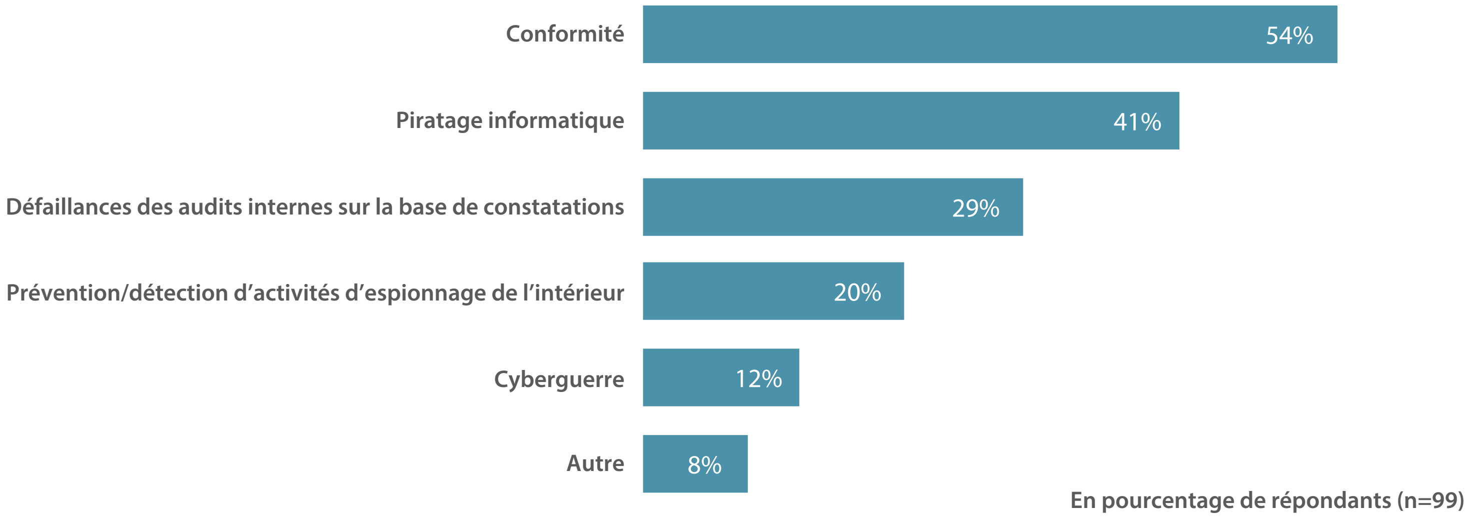
Historiquement, les bases de données ont représenté la grande priorité de l’équation BC/DR et à juste titre. En tant que principal environnement applicatif de l’activité, les bases de données constituent la priorité logique de la protection des données. Mais les temps changent. L’environnement professionnel d’aujourd’hui dépend de plus en plus de documents, d’e-mails et d’autres informations stratégiques qui sont créés, stockés et partagés à l’intérieur de jeux de données Office 365. Ce type d’informations représente une majorité croissante des données locales et distantes, générées et stockées comme une partie essentielle de l’activité moderne.

On peut facilement penser que toutes les protections de données se ressemblent. Or, il existe des différences majeures entre protéger l’infrastructure Office 365 et protéger les données des clients créées et stockées dans Office 365. Par conséquent, il est essentiel que l’IT contribue à établir l'importance métier proportionnée des données Office 365, afin d’assurer une protection et une gouvernance des données appropriées. Si la flexibilité collaborative offerte par le stockage SaaS partagé est un aspect positif, elle ne fait que renforcer l’importance d'une sécurité suffisante à laquelle l'informatique doit contribuer contre les intrusions ciblées.

Cette brèche dans la protection des données n’est pas perdue pour les cybercriminels : ils se consacrent activement aux attaques par ransomware et à d’autres techniques malveillantes capables de tirer parti des écarts et des vulnérabilités entre la responsabilité du fournisseur de SaaS et les entreprises qui détiennent les données. Elle n'échappe pas non plus à l’attention des régulateurs qui donnent de plus en plus la priorité à la sécurité des données. En 2018, une étude de sécurité VoTE de 451 a interrogé les grandes entreprises sur leurs principales préoccupations de sécurité au cours des 90 derniers jours. L'étude souligne que les inquiétudes relatives à la conformité dépassent celles concernant les menaces et les malveillances, ce qui est révélateur.

Figure 3 : Principales préoccupations de sécurité de l'information au cours des 90 derniers jours

Source : 451 Research Voice of the Enterprise : Information Security, Organizational Dynamics 2018
Q : Quelles ont été vos principales préoccupations de sécurité de l'information au cours des 90 derniers jours ?



La plupart de ces préoccupations de sécurité correspondent presque exactement aux vulnérabilités les plus courantes d'Office 365 et d'autres environnements de données partagées. Mais ces risques peuvent être considérablement réduits par un schéma de protection des données basé sur la classique règle du 3-2-1 de la sauvegarde, et planifié de manière à respecter des conditions RTO/RPO appropriées. Les données Office 365 qui se trouvent principalement dans le cloud offrent une commodité et une disponibilité relativement élevées, mais les meilleures pratiques exigent encore de les sauvegarder au moins vers un fournisseur de cloud public tel qu'Azure ou AWS, ou en local, afin d'assurer une meilleure accessibilité et un plus grand contrôle.

Cela nous amène à la raison la plus importante de disposer d'une sauvegarde : la restauration des données. Une sauvegarde Office 365 garantit la protection contre les pertes de données, mais cela n'a que peu de valeur si la restauration est limitée par des facteurs tels que la bande passante, la connectivité, la granularité de la restauration, les défaillances de sauvegarde ou l'incapacité à effectuer des restaurations vers une autre destination ou dans un autre format. Les administrateurs IT qui se penchent sur la protection des données — en particulier dans le contexte des données Office 365 — sont souvent chargés de relever des défis complexes pour restaurer des données spécifiques à partir d'un référentiel de sauvegardes à grande échelle ou des jeux de données Office 365 complets après une attaque par ransomware. Mais les responsabilités des administrateurs peuvent également être aussi ordinaires que la restauration d'un e-mail ou d'un fichier précis pour un utilisateur. C'est pourquoi disposer des outils adéquats pour y parvenir aussi rapidement et efficacement que possible permet de gagner un temps précieux à affecter à des tâches métier plus importantes. En règle générale, à toute stratégie de sauvegarde Office 365 doit correspondre une stratégie de restauration qui tient compte des vulnérabilités de perte de données de toute ampleur, qui offre des options de restauration granulaires et ciblées, ainsi qu'un schéma de vérification évoluant au fil des changements apportés à l'infrastructure, à la plateforme ou aux conditions RTO/RPO.

Archivage, gouvernance et e-discovery Office 365

Bien que très similaires, les sauvegardes et les archives ne sont pas la même chose et doivent être approchées avec des objectifs différents. Dans le cas d'Office 365, l'archivage des données SaaS apporte un modèle de transition et d'administration des données plus anciennes et moins souvent utilisées vers un niveau distinct. Alors que cet archivage permet de configurer des workflows de données basés sur des règles et constitue une manière pratique d'étendre la capacité de stockage en ligne d'Office 365, ce n'est pas un substitut des sauvegardes habituelles. Et bien que les données contenues dans ces archives changent plus lentement, il est important d'assurer que les données archivées sont aussi protégées par une stratégie de sauvegarde de type 3-2-1.

Le risque le plus récent relatif aux données SaaS provient des défis liés aux mesures de confidentialité, telles que le RGPD et le California Consumer Privacy Act de 2018 qui doit entrer en vigueur en 2020. Depuis 2018, le RGPD s'applique au traitement des données à caractère personnel de toute activité commerciale dans l'UE, indépendamment de l'endroit où le traitement a lieu, à l'intérieur ou à l'extérieur de l'UE. Cette réglementation donne aux résidents européens un plus grand contrôle de leurs données. Les prérogatives des individus comprennent la capacité d'interdire le traitement des données au-delà du but spécifié lors de leur collecte, le droit à l'oubli et la possibilité de retirer son consentement au recueil et à l'utilisation des données personnelles.

Cela peut devenir un sérieux problème qui empire avec la quantité colossale d'anciennes données qui s'accumulent dans l'ensemble du secteur. Protéger et administrer correctement tous ces e-mails, documents et sites peut représenter une tâche difficile, mais du point de vue de l'entreprise, il ne faudra pas longtemps avant que les risques de ne *pas* administrer les données personnelles ne dépassent de loin les coûts de correction du problème en cas d'infraction. Le RGPD seul prévoit des sanctions pour non-conformité qui peuvent coûter à une entreprise jusqu'à 20 millions d'euros ou 4 % de son CA annuel mondial, selon la somme la plus importante. Aux États-Unis, la proposition du California Consumer Protection Act de 2018 adopte un modèle différent basé sur une amende de 7 500 $ pour chaque infraction. À titre dd'exemple, une violation du CCPA concernant 500 000 comptes pourrait entraîner une amende de 3,75 milliards de dollars.

Une autre considération légale qui motive la protection des données SaaS est le processus d'e-discovery auquel les entreprises doivent se soumettre dans le cadre d'une action en justice. Quand une entreprise reçoit une citation à comparaître pour produire ses données commerciales, celles-ci deviennent soudain des preuves, ce qui change tout. En fonction de la nature de la demande, il incombe alors à la société d'identifier, de préserver, de recueillir et de traiter ces données pour les présenter à son équipe juridique qui les examinera et les analysera pour juger de leur pertinence et de leur contexte, en exclure les informations légalement non communicables et les préparer à être soumises au tribunal. Une obligation de conservation est un processus de verrouillage des données qui vise à s'assurer qu'elles ne sont pas supprimées ni modifiées, et il est important de disposer des outils nécessaires pour répondre aux besoins de protection granulaire et de sécurité d'un événement d'e-discovery. Mais une obligation de conservation doit être employée de manière sélective, et bien que les offres Office 365 comportent de telles capacités, une copie de sauvegarde complète et indépendante des données SaaS peut constituer la meilleure approche pour fournir un jeu de données datant d'un instant précis pour les besoins de l'e-discovery. Malheureusement, les règles relatives aux preuves sont susceptibles de varier considérablement d'une juridiction à l'autre. Aussi, une entreprise doit toujours consulter un conseil juridique avant de répondre à l'ordonnance d'un tribunal concernant une preuve numérique et suivre ses instructions à la lettre.

Que ce soit sur le plan légal ou autre, nous estimons que les entreprises auront de plus en plus besoin d'une meilleure visibilité et d'un contrôle renforcé de leurs données cloud et SaaS. Avec Office 365, les clients professionnels disposent de commodité alliée à la flexibilité. Y associer un modèle de protection des données prend tout sens, alors que les options de stockage SaaS d'Office 365 continuent à gagner du terrain dans le monde de l'entreprise. Une approche véritablement cloud hybride devrait considérer les services et les ressources de cloud public comme une extension d'une infrastructure locale. De plus, les principes fondamentaux de la protection des données, de la continuité d'activité et de la reprise après incident ne doivent pas s'évaporer simplement parce qu'une application s'exécute dans le cloud.

Conclusions/recommandations

Quand il s'agit d'applications telles qu'Office 365, les fournisseurs de SaaS offrent des assurances raisonnables quant à la protection de leur propre infrastructure pour respecter leurs accords de niveau de services (SLA) contractuels. Mais cette protection ne s'étend pas aux données des clients créées sur ces plateformes. Il est essentiel que les clients trouvent des solutions pour protéger leurs propres données contre les risques — et selon leurs propres conditions plutôt qu'en fonction des limitations potentielles des offres de plateformes SaaS. Le défi actuel des structures IT tient à comprendre les vulnérabilités associées aux données résidant sur les plateformes SaaS et à assurer la mise en place de solutions appropriées de protection, de contrôle et d'accessibilité. Ces actions font partie des mesures capitales à prendre pour envisager de protéger des données Office 365.

- **Gardez à l'esprit que Microsoft assure la résilience de l'infrastructure et la disponibilité des applications dans le cadre d'Office 365, mais, également, que vous êtes le propriétaire des données.** Vous êtes responsable de la protection de vos propres données commerciales et vous devez définir cette protetion en fonction des besoins spécifiques de votre activité.
- **Faites vos recherches et envisagez d'acquérir une solution de sauvegarde des données tierce.** C'est l'une des meilleures manières de protéger votre entreprise contre les vulnérabilités de données relatives à Office 365. Préparez un plan contre les menaces telles que la suppression accidentelle et les failles de sécurité internes et externes, grâce auquel respecter les obligations de sécurité ou de conformité.
- **Incitez les parties prenantes de votre entreprise (et de votre service informatique) à définir et tester les SLA de restauration de données.** Testez divers scénarios de restauration des données dans le cadre des outils natifs des plateformes SaaS et comparez ceux-ci aux produits de sauvegarde tiers.
- **Soyez au fait des règles spécifiques de conformité et des lois de votre environnement professionnel**. Les lois entourant la protection et la sécurité des données changent en permanence et l'une des considérations clés de tout plan de protection des données doit être d'assurer la conformité.

À propos de 451 Research

451 Research est une société majeure de recherche et de conseil en technologies de l'information. Fortement axés sur l'innovation technologique et les bouleversements du marché, nous fournissons des évaluations essentielles aux leaders de l'économie numérique. Plus de 100 analystes et consultants offrent ces perspectives au moyen de recherches communes, de services de conseil et d'événements en direct à plus de 1 000 entreprises clientes en Amérique du Nord, en Europe et partout dans le monde. Fondée en 2000 et basée à New York, 451 Research est une division de The 451 Group.

NEW YORK
1411 Broadway
New York, NY 10018
+1 212 505 3030

SAN FRANCISCO
140 Geary Street
San Francisco, CA 94108
+1 415 989 1555

LONDRES
Paxton House
30, Artillery Lane
London, E1 7LS, UK
+44 (0) 203 929 5700

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

451 Research®