IDC
Analyze the Future

LIVRE BLANC

Critères clés pour sélectionner un prestataire de sauvegarde sur le Cloud construit pour durer

Sponsorisé par : EMC Mozy

Liz Conner Laura DuBois

Mai 2013

DANS CE LIVRE BLANC

Les services Cloud ont un effet transformationnel sur les organisations IT aujourd'hui. Ils changent non seulement la manière dont l'informatique est construite, procurée et déployée mais également de qui et comment l'infrastructure informatique est fournie. Le stockage est une industrie affrontant une perturbation majeure au fur et à mesure que les consommateurs et les entreprises offrent une capacité de stockage et des fonctions à partir des prestataires de services sur le cloud public. Toutefois, ce qui est essentiel pour un déploiement durable et réussi d'un service de stockage sur cloud public est une diligence raisonnable complète du prestataire de cloud offrant le service. Ce papier identifie les critères clés que les entreprises doivent utiliser pour évaluer une société de prestataires de service sur cloud qui est construite pour durer. Il identifie également comment Mozy de EMC Corporation traite ces exigences, permettant à plus de 100 000 clients entreprises et à des millions de particuliers de se fier au Cloud Mozy pour la protection et la récupération de leurs données.

ÉTAT DES LIEUX

L'essor du Cloud et son impact

Les services de Cloud, avec la mobilité, les données/analyses volumineuses et les médias sociaux, sont l'une des quatre technologies transformationnelles de pointe validant les nouvelles stratégies d'entreprise et d'informatique. Les services de Cloud ont changé la manière dont certaines applications se développent ainsi que la manière dont de grandes portions de l'infrastructure informatique sont achetées, gérées et déployées. Ils permettent aux sociétés d'externaliser certaines portions de leurs besoins en matière d'informatique, de stockage et/ou de données, résultant en économies de capital et de coûts d'exploitation pour les budgets informatiques limités. Les services de Cloud permettent aux organisations d'acheter juste ce dont elles ont besoin tout en bénéficiant de services plus facilement mis à niveau et en éliminant le besoin d'approvisionnement excessif en matériel dur en anticipation d'une croissance future. La gestion de l'infrastructure informatique ne peut pas non plus être ignorée. La surveillance continue, le dépannage et la gestion de l'infrastructure et des applications peuvent être déchargés des équipes d'opérations internes et confiés à un prestataire de cloud.

Au fur et à mesure de la croissance du cloud computing, le composant de stockage est à l'avant-garde. Systématiquement, depuis 2006 lors de la première initiation d'IDC de sa recherche de cloud, le stockage est l'un des cas d'utilisation importants pour le cloud

Siège social : 5 Speen Street Framingham, MA 01701 USA Tél. : 508.872.8200 Fax : 508.935.4015 www.idc.com

public. D'après l'Enquête CloudTrack 2012 d'IDC auprès de 493 informaticiens, e-mail antérieur, sauvegarde/archive étaient la charge de travail numéro 2 la plus susceptible de migrer vers le cloud public. Pourquoi ? Pour des organisations recherchant un déploiement rapide d'un stockage accru ou une sauvegarde rehaussée sur ordinateur/ordinateur portable, dans les limites des budgets d'exploitation établis (opex), les services de stockage sur cloud public offrent un stockage relativement aisé, hors site et doté d'une solution de paiement évolutive. Les cas d'utilisation importants pour ces types de déploiements sur les clouds publics et hybrides sont la sauvegarde, le stockage et la récupération des données en cas de catastrophe. En sauvegardant sur le cloud, les organisations opposées aux approches d'investissement peuvent épargner de l'argent sans avoir à créer ni gérer de site de sauvegarde physique avec un stockage physique et ont également une solution de récupération après sinistre intégrée au cas où quelque chose arriverait à leur installation du centre de données principal sur site.

Tandis que la majorité des organisations informatiques continuent de préférer des approches de stockage sur site de confiance — NAS, SAN, etc. — pour des besoins critiques tels que le stockage pour machines virtuelles, base de données et applications transactionnelles, IDC est convaincue que la sauvegarde et la récupération après sinistre vont continuer d'être les facteurs clés dans l'essor du cloud computing. Parmi les 163 informaticiens et professionnels du stockage interrogés lors de l'Enquête d'IDC Disk-Based Data-Protection de mars 2012, approximativement 64,5 % des entreprises utilisent ou prévoient d'utiliser une stratégie de sauvegarde sur cloud public. Cette même enquête souligne que des 38 % utilisant actuellement le cloud public pour sauvegarde, celui-ci est pour un pourcentage relativement petit mais croissant de leur volume total de données.

Néanmoins, au fur et à mesure que le cloud computing, et avec lui la sauvegarde sur le Cloud, devient plus populaire, nous commençons à voir des distinctions entre les divers types de services et de prestataires de sauvegarde sur le Cloud, alors que les fournisseurs se taillent de nouveaux marchés cibles et que des groupes différents requièrent une sauvegarde sur le Cloud avec différents attributs.

- **Consommateur c. entreprise :** il existe des distinctions évidentes entre les besoins des consommateurs et des entreprises, visibles dans la capacité de stockage nécessaire, le support d'application nécessaire, le besoin d'outils administratifs et la fonctionnalité, la disponibilité de bande passante pour satisfaire au volume de données, le nombre d'utilisateurs, les fonctions de sécurité requises, l'assistance à la clientèle, la disponibilité et les modèles de paiement (freemium c. abonnement payant). Bien que les exigences des consommateurs ne doivent pas être prises à la légère, les entreprises clients ont besoin d'un prestataire qui soit adepte à traiter les besoins spécifiques d'entreprise. Les besoins spécifiques d'entreprise englobent typiquement des exigences sur la sécurité, la sûreté, la confidentialité et l'emplacement des données, le support des applications/l'assistance à la clientèle, le traitement efficace de gros volumes de données, et des services d'appui qui peuvent passer sur des réseaux partagés ou privés, de point à point.
- **Start-up c. prestataire établi :** les services de Cloud représentent la croissance de l'industrie informatique et offrent des barrières relativement basses à l'entrée de nouvelles sociétés innovantes. Résultat : les petites start-ups ciblent et vont continuer

de cibler les marchés à créneaux qui sont actuellement mal desservis ou tenter de fournir un service distinct/nouveau, modèle de tarification, fonctionnalités, etc. Pour minimiser les coûts de start-up, un grand nombre utilise une infrastructure de tierce partie comme service (IaaS) plutôt que d'établir leur propre matériel dur. Par conséquent, un service de cloud peut dépendre d'une tierce partie pour satisfaire aux SLA et le dépannage peut être complexe. Inversement, les prestataires de cloud établis ont tendance à créer et exploiter leurs propres clouds, ciblant soit la population des consommateurs soit le monde général des commerces/entreprises soit, dans certains cas, les deux. Les prestataires de cloud établis ont réussi les processus de certification et d'audit, et possèdent également une expérience précieuse dans le déploiement et la gestion de l'infrastructure de cloud. Le prestataire établi peut également proposer des SLA plus riches, des offres plus personnalisées ainsi que la viabilité commerciale et financière absente dans les offres des start-ups.

La sauvegarde sur cloud public est devenue une partie intégrale accrue de l'informatique d'entreprise. Un grand nombre de facteurs différents contribue à distinguer les offres des différents prestataires. D'après la prévision de stockage dans le cloud d'IDC, IDC estime que le marché des services de sauvegarde sur cloud public atteindra plus de 2 milliards de dollars en dépenses en 2013 et voit un taux de croissance annuel composé (TCAC) de 33 % de 2010 à 2015, pour atteindre plus de 3,6 milliards de dollars en dépenses d'ici 2015. Avec des dépenses matérielles sur les services de cloud public pour sauvegarde l'emportant dramatiquement sur le TCAC plus modeste de 4,8 % pour le marché des logiciels de sauvegarde de données sur place classique, choisir le bon prestataire de service n'a jamais été aussi important, surtout avec une fonction telle que la sauvegarde qui est notoirement de longue durée en termes de données, de format et d'empreinte.

CRITÈRES DE SÉLECTION D'UN PRESTATAIRE DE SAUVEGARDE SUR CLOUD

Pour que les organisations entreprises puissent déterminer quel prestataire de sauvegarde sur cloud convient le mieux à leurs besoins, il est important d'établir certains critères auxquels doit satisfaire un prestataire potentiel. Les critères suivants sont les fonctions principales à évaluer lors de la sélection d'un prestataire de sauvegarde sur cloud. Ces critères peuvent être utilisés par des firmes qui procèdent à leur propre analyse des prestataires de services, des offres et des accords contractuels.

Société de prestataires de service sur cloud qui est construite pour durer

Étant donné la nature de la sauvegarde sur cloud, un prestataire de sauvegarde sur cloud doit y être au long terme. Bien que les start-ups et même les acteurs établis puissent présenter des économies de coûts initiales ou des fonctions uniques, s'ils doivent disparaître de la circulation dans les cinq années à venir, ils représentent une énorme responsabilité pour leurs clients potentiels. Lorsqu'une firme utilise un serveur sur site ou du matériel de stockage, si le fournisseur informatique cesse ses activités, les clients n'ont plus de société à appeler pour la maintenance/le service et doivent, éventuellement, déplacer leurs applications ou les données stockées dans un système différent. Néanmoins, cette transition peut généralement se faire selon

les besoins et, si la migration réussit, sans perte de données associée à la sortie d'une société de matériel de stockage. On ne peut pas en dire autant d'un prestataire de cloud. Lorsque les prestataires de cloud quittent le marché, il y a un risque qu'ils le fassent avec les données de leurs clients, résultant en préoccupations potentielles de sécurité, perte de données et visibilité des parties prenantes de l'entreprise. Pour s'assurer qu'un prestataire de sauvegarde sur cloud est construit pour durer, les clients potentiels doivent examiner de près les catégories suivantes.

- Stabilité financière : Si le prestataire de cloud ne se trouve pas dans une situation financière rentable ou s'il essaie toujours d'établir un modèle d'entreprise prospère et/ou une base de clientèle, il y a un haut niveau de risque que cela sera une entreprise qui ne réalisera jamais de profits et que la société fermera ses portes. Questions à poser pour vérifier la stabilité financière d'un prestataire de service incluent (les réponses peuvent être divulguées sous un accord de non-divulgation signé) :

  - Êtes-vous rentable aujourd'hui ? Si non, quand prévoyez-vous de l'être ?
  - Quelle est votre situation de trésorerie ?
  - Quelle est votre cote de solvabilité actuelle ?
  - Pouvez-vous fournir une copie signée des relevés financiers audités les plus récents de votre société ?
  - Votre société a-t-elle demandé la protection de la loi sur la faillite ? Quand ? Pourquoi ?

- **Infrastructure éprouvée :** Bien qu'une technologie innovante et un matériel dur puissent permettre de moderniser une industrie ou d'établir de nouvelles industries, dans le cas de la sauvegarde sur cloud, l'infrastructure implémentée par le prestataire de cloud doit être un prestataire éprouvé pour qu'un client entreprise confie au prestataire de cloud des données d'entreprise critiques. Comme mentionné préalablement, de nombreux services de sauvegarde sur cloud peuvent se fier aux IaaS de tierce partie et sont, par conséquent, dans une relation dépendante pour satisfaire aux ANS ou dépanner les problèmes. Les questions à poser pour établir si le prestataire de service utilise une infrastructure éprouvée incluent :

  - Exploitez-vous un modèle acheter-et-exploiter, ou dépendez-vous de prestataires IaaS ?
  - Dans l'un ou l'autre des cas, quels sont les ANS de disponibilité de service, résilience, réussite de sauvegarde, temps de sauvegarde, temps de restauration, etc. ?
  - Les ANS sont-ils documentés et publiés ?
  - Pour les prestataires de service qui utilisent du matériel dur et un logiciel commerciaux plutôt que de construire l'infrastructure elle-même, quelle infrastructure de matériel et de logiciel est-elle utilisée ?

- Depuis combien de temps cette infrastructure est-elle en production ?

- **Base de clientèle établie :** Lors de la recherche d'un prestataire, il est utile de savoir quelles autres entreprises utilisent actuellement les services du prestataire. Une petite base de clientèle, bien que croissante, indiquerait plus d'une start-up. Une perte de base de clientèle indiquerait que quelque chose ne va pas et fait partir les clients. Assurez-vous que les prestataires de service qui cotent des milliers ou des millions de clients font référence à des clients commerciaux pas seulement des consommateurs. De nombreux prestataires de service commencent par un consommateur ou un focus SMB mais peuvent ne pas être encore des prestataires d'entreprise établis. Pour minimiser le risque, recherchez un prestataire ayant une grande clientèle d'entreprises. Utilisez votre réseau interne ou de pairs pour parler aux clients d'un prestataire de service quelconque. Les questions à poser incluent :

  - Combien de consommateurs utilisent votre service à l'heure actuelle ? Ces clients sont-ils des clients freemium ou payants ?

  - Combien d'entreprises utilisent votre service à l'heure actuelle ? Sont-elles des PME ou des clients d'entreprises ?

  - Quelle croissance avez-vous vue dans chaque secteur au cours des 12 ou 24 mois passés ?

  - Depuis combien de temps desservez-vous des clients entreprises ?

  - Y a-t-il des clients qui ne conviennent pas à votre service ? Lesquels ? Pourquoi ?

- **Centres de données répartis géographiquement :** comme l'ouragan Sandy en 2012 l'a montré, il est utile que le centre de données sur cloud qui détient les fichiers de sauvegarde ne se trouve pas à 40 km le long de la côte (en cas de sinistre naturel). Les centres de données répartis géographiquement deviennent importants pour garantir qu'il existe des basculements si une disponibilité constante est requise et qu'il existe un problème inattendu avec le centre de données principal où se trouvent les données. L'emplacement est important pour diversifier les risques, surtout dans le cas de catastrophes naturelles mais également pour se conformer aux exigences de juridiction régionale pour l'emplacement des données. Par exemple, certaines géographies ont des exigences selon lesquelles les données ne sortent pas des frontières régionales, ce qui nécessite qu'un prestataire de service ait des installations physiques dans cette région. Même si le respect des lois locales sur le traitement des données par le fournisseur du nuage représente un critère important, la mesure la plus importante des capacités du fournisseur en matière de sécurité des données comprend sa prise en charge des niveaux de cryptage adéquats pour les données ainsi que leur confidentialité garantie, comme indiqué dans la section Service par des pratiques avancées en matière de sécurité et de confidentialité. Les questions à poser incluent :

  - Vos centres de données sont-ils géographiquement répartis ou avez-vous des centres de données en dehors des États-Unis pour les clients situés en Europe ou Asie/Pacifique, par exemple ?

- Pouvez-vous me garantir que mes données iront à un centre de données particulier ?

- Quel est votre plan de continuité commercial en cas d'échec du site ou d'exploitation ?

- **Validation et accréditation de tierce partie :** des audits réussis et périodiques des procédures de sécurité du prestataire de sauvegarde sur cloud sont essentiels pour vérifier que le traitement et l'accueil du prestataire de cloud des données du client se font de manière sûre et sécuritaire. SSAE 16 est une norme d'audit largement reconnue développée par l'American Institute of Certified Public Accountants (AICPA) qui vérifie qu'une organisation a fait l'objet d'un audit approfondi de ses objectifs et activités de contrôle afin de garantir que le traitement et l'hébergement des données des clients se font de manière parfaitement sécurisée. En outre, la certification ISO 27001 établit un prestataire de cloud potentiel comme ayant satisfait aux normes internationales pour l'évaluation des systèmes de gestion de la sécurité des informations. ISO 27001 définit des exigences et meilleures pratiques pour une approche méthodique de la gestion des informations des entreprises et des particuliers. Elle repose sur des estimations périodiques des risques adaptées aux menaces en perpétuelle évolution. Voyez si votre prestataire de service a les réponses aux questions suivantes :

  - Avez-vous déjà subi des audits de sécurité de tierce partie au cours des derniers 24 mois ? Par qui et quand ?

  - Veuillez fournir les résultats de ces audits.

  - Votre entreprise possède-t-elle des certifications ISO 27001 ou ISO 27002, SSAE 16, PCI DSS, HIPAA ou autres ?

- **Termes et exécution d'un ANS :** Les termes et l'exécution d'un ANS établis sont intégrés non seulement pour établir la manière dont les données d'un client seront traitées et entreposées mais également pour établir un niveau transparent de service sur lequel le client peut compter de la part du prestataire de cloud. Ceci permet d'établir des niveaux d'attente et d'établir le niveau anticipé de service. Les questions à poser à votre prestataire de service incluent :

  - Comment sont surveillés et évalués les ANS, et par qui ?

  - Y a-t-il des interruptions d'activité que ces ANS ne couvriraient pas ? Veuillez fournir une description.

Service créé sur les pratiques de sécurité et de confidentialité de pointe

L'une des principales préoccupations de la sauvegarde sur cloud est la sécurité et la confidentialité des données. Les sociétés se préoccupent des intrusions extérieures illégales dans leurs données (autrement dit, piratage), de la saisie potentielle du matériel dur du prestataire de cloud par les autorités gouvernementales et des prestataires de cloud utilisant un accès non autorisé aux données afin d'exploiter les

statistiques ou de vendre les données. Étant donné que les données de sauvegarde ne sont pas physiquement sous le contrôle de l'entreprise, les préoccupations de sécurité et de confidentialité seront toujours à l'avant-plan du département informatique de l'entreprise. Par conséquent, il est essentiel qu'un prestataire de cloud offre ce qu'il y a de mieux en matière de sécurité et de confidentialité. Les fonctions de sécurité essentielles pour un client entreprise incluent :

- **Cryptage AES à clé personnelle :** La capacité pour les clients de configurer et de maintenir leurs propres clés de cryptage personnel qu'ils, non pas le prestataire de service, contrôlent. AES est jugé la norme du cryptage, étant utilisé par diverses agences gouvernementales et étant certifié FIPS. Plus important, la capacité pour les clients d'établir et de gérer leurs propres clés de cryptage signifie que les prestataires de sauvegarde sur cloud ne peuvent pas décrypter leurs fichiers et ce, même obligés par la loi.

  - Votre organisation a-t-elle un programme de sécurité d'information officiel, documenté, mandaté et dans toute la société, y compris des politiques de sécurité, des normes et procédures ? Veuillez les indiquer.

  - Exigez-vous que les données soient cryptées durant les sauvegardes ? À quel niveau de cryptage ?

- **Cryptage sur le réseau et au repos :** S'assurer que les données sont cryptées lorsqu'elles sont transférées vers les prestataires de sauvegarde sur cloud (sur le réseau) et pendant qu'elles sont stockées au sein des systèmes de prestataires de sauvegarde sur cloud (au repos). L'utilisation combinée de ces deux types de cryptage permet d'établir une sécurité de données plus forte qu'un seul type. Bien sûr, le cryptage doit se faire de concert efficace avec des stratégies efficaces de stockage telles que la compression et la déduplication.

- Gestion/Manipulation de clé : Établissement de la personne contrôlant la clé de cryptage, que la gestion/connaissance de la clé réside avec le prestataire de sauvegarde sur cloud ou que le client maintienne l'ensemble de la gestion et de la connaissance de la clé de cryptage. Si la gestion de clé réside avec le client, le prestataire de sauvegarde sur cloud doit avoir un processus en place pour s'assurer que la clé de cryptage est entreposée localement avec le client et non pas sur le système du prestataire sur cloud. Des niveaux variés de gestion de clé sont recommandés pour répondre aux besoins divers des clients.

  - Demandez aux prestataires de service de décrire l'infrastructure de manipulation des clés de cryptage de leurs organisations.

  - Demandez aux prestataires de service de décrire les options de leurs organisations pour manipuler les clés cryptage.

- **Programme de sécurité documenté, mandaté et surveillé :** Assurez-vous que le prestataire de cloud a un programme de sécurité en place et qu'il est bien documenté et répond à tous les mandats. Ceci permettra d'établir la crédibilité en matière de sécurité du prestataire de cloud.

  - Les politiques de sécurité sont-elles documentées ?
  - Le prestataire de service dispose-t-il d'une organisation de sécurité attitrée ?
  - A-t-il subi une évaluation de vulnérabilité par une tierce partie reconnue ? Pouvez-vous fournir les résultats ?

En termes de préoccupations de confidentialité, les fonctions de confidentialité clés suivantes sont celles que les entreprises devraient rechercher chez un prestataire de sauvegarde sur cloud potentiel :

- **Politiques sur la confidentialité des données documentées, mandatées et surveillées :** les entreprises clients veulent s'assurer que les fournisseurs de sauvegarde sur le cloud ont des politiques en place pour traiter toute question de confidentialité. Ceci permettra d'établir la crédibilité des fournisseurs de cloud alors qu'ils prennent le temps d'établir et de documenter les politiques de confidentialité. Les questions à poser à un prestataire de cloud incluent :

  - Disposez-vous d'une politique de confidentialité publiée et accessible au personnel ? Est-elle révisée et approuvée par un comité du conseil ?
  - Permettrez-vous à une société indépendante de vérifier vos procédures de confidentialité ?

- **Politique sur l'exploitation de données/publicité du client :** les prestataires de cloud doivent être transparents avec leur politique sur l'utilisation des données du client — que le prestataire de cloud y ait accès à des fins de publicité et/ou d'exploitation des données ou que l'accès aux données soit strictement interdit à tous sauf pour le client. Les sentiments des entreprises concernant l'utilisation à des fins de publicité/d'exploitation des données vont varier, mais les prestataires de cloud doivent être francs et transparents dans leurs politiques concernant leur utilisation des données de client.

  - Veuillez expliquer vos politiques sur l'utilisation des données du client pour publicité ou exploitation de ces données pour des gains monétaires.

- **Pratiques de sauvegarde d'informations confidentielles ou sensibles :** certaines données, plus que toutes les données, sont du type confidentiel ou sensible. Ce type de données requiert des protocoles de sécurité additionnels. Les prestataires de cloud doivent avoir une pratique établie pour sauvegardes additionnelles concernant du matériel sensible.

  - Avez-vous des procédures mises en œuvre pour s'assurer que le personnel et les sous-traitants maintiennent la sécurité et la confidentialité de vos données ? Veuillez décrire.

TABLEAU 1

Liste de vérification des fonctions de sauvegarde sur cloud clés

	Fonctions de Mozy
Construit pour durer	
Stabilité financière	Mozy est un service de cloud offert par EMC, une entreprise cotée en bourse de 47 milliards de dollars.
Infrastructure éprouvée	Les services cloud Mozy fonctionnent depuis plus de huit ans. L'infrastructure de sauvegarde durcie inclut 90 Po de données sur cloud sous gestion.
Base de clientèle établie	Mozy a plus de 100 000 entreprises clients et plus de 6 millions d'utilisateurs finaux de ses services. Mozy fournit des services de sauvegarde sur cloud à des entreprises clients depuis 2008.
Emplacements de centres de données répartis géographiquement	Mozy a un réseau de centres de données réparties géographiquement y compris des centres de données aux Amériques et en EMEA pour les clients et partenaires dans ces régions.
Certifications	Mozy est certifié ISO 27001 et conforme à la « Sphère de sécurité ».
Audits réussis	Mozy a réussi un audit SSAE 16 Type II.
Termes et exécution d'un SLA	Mozy gère à une disponibilité de service des trois neufs.
Sécurité	
Cryptage AES à clé privée	Mozy offre un cryptage AES privé avec sa clé personnelle et une clé de client entreprise.
Cryptage sur le réseau et au repos	Toutes les données sont cryptées pendant le processus de sauvegarde, envoyées sur une connexion SSL cryptée et cryptées au repos pour une protection complète de données de bout en bout.
Gestion/manipulation de clé	Mozy offre trois niveaux de gestion de clé : une clé par défaut, utilisant Blowfish et gérée par Mozy ; une clé personnelle, utilisant AES et gérée par le particulier ; et une clé personnalisée d'entreprise, utilisant AES et gérée par le client entreprise.
Sécurité du personnel	Mozy a un programme de sécurité personnelle en place qui inclut des vérifications de casier judiciaire, la gestion d'accès et l'audit.
Programme de sécurité documenté, mandaté et surveillé	Mozy a un système de gestion de la sécurité de l'information ISO en place.
Politiques de sécurité	Mozy a une équipe de sécurité de cloud attitrée qui développe et maintient des politiques de sécurité physiques et numériques exhaustives. Les politiques de sécurité de Mozy peuvent être partagées avec des clients selon les besoins.
Simulations d'intrusions et évaluations de vulnérabilité	L'évaluation de vulnérabilité est effectuée tous les trois mois ou selon les besoins. Les simulations d'intrusions sont effectuées par l'équipe de sécurité Mozy selon les besoins à l'appui du programme d'évaluation de vulnérabilité.

TABLEAU 1

Liste de vérification des fonctions de sauvegarde sur cloud clés

	Fonctions de Mozy
Protection des données personnelles	
Politiques sur la confidentialité des données documentées, mandatées et surveillées	La politique de confidentialité de Mozy est documentée sur son site Web (disponible à mozy.com/privacy).
Politique sur la publicité de l'utilisateur/accord de ne pas exploiter les données de client pour publicité	Mozy ne vend ni ne commercialise les données d'utilisateur et ne visualise pas les données de sauvegarde des utilisateurs finaux.
Pratiques de sauvegarde d'informations confidentielles ou sensibles :	Mozy a des politiques de classification et de manipulation des données, ainsi que des procédures de traitement des informations qui définissent divers niveaux de classification de données et les contrôles associés à ces niveaux.
Conformité avec les règlementations locales et régionales sur la confidentialité des données	Mozy est conforme à la « Sphère de sécurité » et offre un réseau de centres de données géographiquement répartis.
Un service créé avec une gestion de données de première classe	
Gestion centralisée	Mozy offre une console d'administration Web partagée au sein d'une architecture mutualisée pour la gestion des comptes par un personnel administratif et sous-administratif. Le logiciel Mozy peut être configuré, déployé et centralement géré via la console d'administration, qui offre des contrôles de configuration personnalisée exhaustifs.
Gamme de clients et d'applications prise en charge	Mozy prend en charge toute une gamme d'applications, y compris les partages réseau, toutes les versions de SQL et Exchange, SharePoint, Active Directory, COM+ services, répertoire partagé SYSVOL et bases de données du registre Windows.
Intégration à Active Directory	Mozy offre une intégration à Active Directory qui déclenche automatiquement la création, l'organisation et la suppression des utilisateurs dans MozyEnterprise.
Gamme de services	Mozy offre une sauvegarde sur cloud consommateurs, une sauvegarde sur cloud commerces (utilisateur final et serveur) et une sauvegarde sur cloud entreprises.
Politiques de sauvegarde et de rétention	MozyEnterprise offre une politique de rétention de 90 jours.
Amorçage : Première sauvegarde	Mozy offre Mozy Data Shuttle, un dispositif pour amorcer la sauvegarde initiale dans le Mozy cloud.
Option hybride pour récupération locale et temps le plus rapide de récupération	Mozy 2xProtect permet d'effectuer une sauvegarde locale sur une unité USB ou un disque externe en outre de la sauvegarde sur cloud. En outre, les solutions de sauvegarde sur site complémentaires BRS sont optimisées pour une sauvegarde sur

TABLEAU 1

Liste de vérification des fonctions de sauvegarde sur cloud clés

	Fonctions de Mozy
	cloud hybride.

Source: IDC, 2013

DÉFIS/OPPORTUNITÉS

Au fil des ans, Mozy s'est établi comme un prestataire de sauvegarde sur cloud de pointe avec des clients consommateurs et entreprises. Mozy a fait preuve de diligence pour répondre aux préoccupations clés que tous les clients ont en matière de cloud public, de confidentialité des données et de sécurité. L'introduction de fonctions telles que le cryptage AES, la gestion de clé privée, l'accès et la connexion, les pistes d'audit, la certification ISO 27001, l'audit SSAE 16 et les nombreux emplacements des centres de données a permis à Mozy d'établir une forte réputation parmi les prestataires de cloud.

Le niveau suivant de distinction se produit avec le raffinement de la manière dont les données sont efficacement déplacées, stockées et récupérées. Se pencher sur la question de la taille d'un volume de données par opposition au pipeline de données utilisé pour les déplacer va accentuer le besoin de technologies d'efficacité de stockage. Un autre défi se révèle dans différentes charges de travail éventuellement requérant différentes options de récupération pour récupérer les données le plus efficacement. Une gamme d'options devrait être mise en œuvre pour résoudre ceci. En répondant à ces préoccupations, Mozy a l'occasion de fournir des services à valeur ajoutée sur lesquels peu d'entreprises se concentrent et, une fois encore, montrer pourquoi il est numéro un en matière de sauvegarde sur cloud.

CONCLUSION

Au fur et à mesure que les organisations entreprises modernisent leurs centres de données de la manière la plus économique et la plus efficace possible, une opportunité continue d'évoluer pour les services de sauvegarde sur le cloud. Pour réduire les coûts des centres de données, particulièrement le matériel de stockage, l'empreinte de bâtiment et les coûts d'alimentation électrique et de refroidissement, les entreprises consultent des prestataires de cloud public pour des services de sauvegarde de données hors site et de récupération en cas de catastrophe. Au fur et à mesure que s'accroît l'intérêt des entreprises dans la sauvegarde sur le cloud, de même le besoin d'un prestataire de cloud compétent s'accroît. Une concentration améliorée sur les besoins propres à l'entreprise, tels que fonctions de confidentialité et de sécurité extensives, gestion de comptes simplifiée et administration multi-utilisateurs, assistance 24 x 7, et évolutivité, établit Mozy comme prestataire de sauvegarde sur le cloud numéro un de l'industrie qui doit se trouver sur la courte liste de prestataires de cloud d'une entreprise.

Notification sur le copyright