MIT Technology Review Insights

Produit en association avec

VEEAM

Les entreprises qui intègrent des technologies cloud font face à de nouvelles complexités en matière de gestion des données.

Le succès du cloud hybride repose sur la protection des données

Principaux points à retenir

1. Le cloud hybride, c'est-à-dire l'offre intégrée de services locaux, de cloud public et de cloud privé, est en passe de devenir le nouveau modèle économique de référence. Les dirigeants d'entreprise sont en train de repenser leur stratégie opérationnelle.
2. Si le cloud hybride propose des outils novateurs en matière de sécurité et de protection des données, il accroît également la complexité et les risques. Les entreprises doivent donc suivre de près l'évolution des pratiques de cybersécurité.
3. Les entreprises doivent moderniser leur stratégie interne de sécurisation et de protection des données. Les attaques sont imprévisibles et onéreuses, avec un coût moyen par incident de cybersécurité atteignant 3,6 millions de dollars.

Après l'acquisition de CA Technologies en 2018 et de Symantec Enterprise en 2019, le fabricant de puces électroniques Broadcom a décidé d'investir dans les environnements de cloud hybride, qui intègrent et orchestrent des services locaux, de cloud public et de cloud privé. Ces acquisitions avaient conduit à une forte hétérogénéité des piles technologiques et des workflows opérationnels, ainsi qu'à la multiplication des scénarios d'hébergement : sur site, en colocation et en mode « natif cloud » (quand l'infrastructure complète réside dans le cloud).

« Nous avons modernisé les logiciels natifs cloud au moyen d'une architecture de conteneurs et microservices que nous avons migrée dans le cloud. Ensuite, nous avons modernisé les datacenters sur site et en colocation au sein de l'architecture de cloud hybride », déclare Andy Nallappan, directeur technique chez Broadcom. Souhaitant intégrer ses acquisitions au sein d'une pile technologique unifiée, tout en continuant d'accorder la priorité aux besoins de la clientèle, à la sécurité et à la conformité, Broadcom devait mener un travail de modernisation, de standardisation, de sécurisation et de déploiement à grande échelle.

De l'avis de Dave Russell, vice-président de la stratégie grandes entreprises chez Veeam, l'engouement pour le cloud hybride se répand dans tous les secteurs comme une traînée de poudre. « Ces dernières années, la pandémie et la conjoncture macroéconomique en résultant ont contraint les entreprises à repenser leur stratégie opérationnelle et à accélérer leur passage au cloud hybride », explique-t-il.

Le marché du cloud hybride va poursuivre son essor rapide,

21,6 %

de TCAC jusqu'en 2026.

Source : Mordor Intelligence

Et les statistiques lui donnent raison : Mordor Intelligence prévoit que le marché du cloud hybride va poursuivre son essor rapide, avec un taux de croissance annuel composé (TCAC) de 21,6 % jusqu'en 2026.

Les entreprises sont de plus en plus nombreuses à opter pour le cloud hybride, qui s'avère une solution à la fois économique, évolutive et flexible dans une optique d'innovation. « L'un des principaux avantages du cloud hybride est qu'il minimise le coût d'expansion de l'infrastructure sur site », explique Kateryna Dubrova, analyste des réseaux et services IoT chez ABI Research, un cabinet international expert en technologies. « En simplifiant le développement du workload dans le cloud, il permet d'accélérer la mise à l'essai, la création de prototypes et le lancement de nouveaux produits. »

Mainmise sur vos données

Face à l'adoption croissante du cloud hybride, la sécurité et la protection des données se retrouvent au centre des préoccupations. « Le problème réside aujourd'hui dans la prolifération des données, des applications et des emplacements », souligne Alexey Gerasimov, vice-président et responsable cloud chez Capgemini Americas. « En effet, ce sont autant de cibles potentielles d'attaque, de pénétration et d'exfiltration de données : non seulement la surface d'attaque est beaucoup plus grande, mais les actifs menacés sont également beaucoup plus nombreux. »

Protéger les données s'avère complexe dans les environnements hybrides. Si les entreprises utilisent souvent plusieurs systèmes provenant d'éditeurs différents, cette approche contribue à la vulnérabilité des données, compromet l'efficacité et augmente les frais généraux. Pour protéger les actifs face à la recrudescence et à l'évolution des menaces de cybersécurité, il est impératif qu'elles comprennent les défis de données inhérents au cloud hybride.

Les entreprises qui exploitent les technologies cloud partent parfois du principe qu'il incombe aux fournisseurs de cloud d'assurer la sécurité et la protection des données. Toutefois, c'est à l'entreprise que revient la responsabilité finale d'instaurer une stratégie de gestion de leurs données — où qu'elles se trouvent. « Comparativement à l'IT classique, la sécurité et la protection du cloud relèvent d'un partage des responsabilités. Le fournisseur de services cloud est responsable de l'infrastructure sous-jacente (services de cloud computing, etc.), tandis que l'entreprise prend en charge la sécurité et la protection des applications, des données et des utilisateurs », précise Kateryna Dubrova.

Ce mode de fonctionnement reprend le principe d'une location de voiture, comme l'illustre Dave Russell : l'agence de location fournit le véhicule avec le plein d'essence, mais c'est au conducteur qui prend le volant d'éviter les accidents. « C'est la même chose avec le cloud hybride : l'infrastructure de travail (racks serveur) est fournie à l'entreprise, qui n'en demeure pas moins responsable de la protection de ses données », conclut-il. « Il incombe bel et bien à l'entreprise de renforcer l'accès aux ports et aux informations d'identification, parmi les nombreux autres paramètres de sécurité à respecter en environnement de cloud hybride. »

Dès lors qu'on en comprend les tenants et les aboutissants, cette responsabilité représente un avantage pour l'entreprise. « De mon point de vue, le cloud hybride convient mieux aux structures assujetties à d'importantes exigences de conformité et de contrôle des données », déclare Andy Nallappan.

67 %

des entreprises utilisent des services cloud dans le cadre de leur stratégie de protection des données.

Source : Veeam Technologies, rapport sur les tendances de la protection des données en 2022

Importance de la reprise après incident

Le cloud hybride offre l'occasion d'améliorer les stratégies de sauvegarde, de restauration et de reprise après incident (DR). Ayant mené l'enquête auprès de plus de 3 000 dirigeants d'entreprise et décideurs IT afin d'établir son rapport sur les **tendances de la protection des données en 2022**, Veeam a constaté que 67 % des entreprises utilisent des services cloud dans le cadre de leur stratégie de protection des données.

Toutefois, la nature distribuée du cloud hybride ne leur permet pas d'obtenir facilement une vue d'ensemble des données et applications en leur possession, indispensable à la solidité de tout plan de protection des données : l'équipe IT ne peut pas réagir aux anomalies qu'elle ne voit pas. L'environnement hybride multiplie les variables de risque et exige l'élaboration de plans distincts de protection des données et de DR afin de parer aux défaillances des services locaux, de cloud privé et de cloud public.

La nature connectée du cloud hybride accroît également le risque et la complexité. En effet, sa flexibilité et sa disponibilité élargissent les possibilités de défaillance ou de violation. « Nous possédions des datacenters aux quatre coins du monde — en Europe, aux États-Unis, en Australie, au Canada », explique Andy Nallappan. « Chacun d'eux nécessitait son propre plan de sauvegarde et de DR. »

Dave Russell regrette que le secteur ait la mémoire aussi courte quant aux conséquences d'une restauration des données inadéquate. Si le séisme et le tsunami qui ont frappé les côtes du Tohoku au Japon en 2011 ont renforcé l'importance des plans de DR et de continuité d'activité, les enseignements tirés sont tombés aux oubliettes en quelques mois à peine. Et Dave Russell de poursuivre : « Investissez dans des processus de sauvegarde et de restauration des données. Inutile d'attendre une fuite de gaz pour se demander si la maison est équipée d'un système de détection. »

« La mise à disposition d'un tableau de bord et d'un panneau de contrôle unique est une demande qui se perpétue probablement depuis que le conseil en gestion existe. »

Alexey Gerasimov, vice-président et responsable cloud chez Capgemini Americas

La restauration est un processus complexe aux multiples composantes, qui s'appuie sur l'automatisation pour réduire les temps d'arrêt en cas de panne. Les fonctions d'automatisation et d'orchestration atténuent la complexité des plans de DR à la demande et fournissent des informations en temps réel sur l'état du système. « La mise à disposition d'un tableau de bord et d'un panneau de contrôle unique est une demande qui se perpétue probablement depuis que le conseil en gestion existe », assure Alexey Gerasimov. « Il se passe tellement de choses qu'il est physiquement impossible de tout gérer manuellement. L'automatisation intervient en coulisses pour capturer, enregistrer, analyser et produire des résultats qui vous donnent un état des lieux précis. »

Outre les scénarios de DR, l'automatisation est essentielle au quotidien. « C'est le pilier de la gestion du cloud hybride », explique Kateryna Dubrova. « Les services d'automatisation fournissent des schémas ou des modèles reposant sur une méthodologie éprouvée. Sans modèles et sans automatisation suffisante, les développeurs devraient écrire un jeu d'instructions spécifique à la gestion des différents workloads dans chaque environnement de travail. Une approche aussi compliquée prend vite une tournure chaotique. »

Déplacement des données

Grâce à un cloud hybride efficace, il est possible de déplacer les données de manière agile et économique entre les ressources locales, le cloud public et le cloud privé. Néanmoins, ce transfert de données accroît la complexité et les risques. « Tout le monde accède aux données de n'importe où. Outre les actifs traditionnellement hébergés en datacenter, les entreprises doivent aussi protéger désormais le datacenter, le cloud et les données en cours de transfert », poursuit Alexey Gerasimov.

La localisation et le déplacement des données font naître des préoccupations en matière de conformité, non seulement dans les secteurs hautement réglementés comme la finance ou la santé, mais également pour toutes les entreprises qui réalisent des transactions transfrontalières. La réglementation en vigueur dans l'Union européenne (Règlement général sur la protection des données, RGPD) ou aux États-Unis (California Privacy Rights Act) exige des entreprises qu'elles structurent et déploient leurs applications conformément aux lois sur les données géolocalisées.

> « Investissez dans des processus de sauvegarde et de restauration des données. Inutile d'attendre une fuite de gaz pour se demander si la maison est équipée d'un système de détection. »
>
> Dave Russell, vice-président de la stratégie grandes entreprises chez Veeam

3,6 $ millions

Coût moyen d'une violation de cybersécurité

Source : Forum économique mondial, rapport « Global Cybersecurity Outlook 2022 »

La protection des données en circulation devrait figurer en tête des priorités lors de l'élaboration d'un plan de cloud hybride. « Dans la mesure où les données seront toujours l'actif le plus précieux des entreprises, le chiffrement des données sur la cible et en cours de transfert peut contribuer à réduire le risque de perte ou de vol dans le cas où un pirate réussirait à exploiter des failles de sécurité », précise Kateryna Dubrova. « La pratique actuelle du chiffrement de bout en bout doit être standardisée et mise en œuvre dans les stockages cloud publics comme privés. »

Stratégies de données

À mesure que l'adoption du cloud hybride s'accélère et que les surfaces d'attaque s'étendent, il est impératif que les entreprises modernisent leur stratégie de sécurisation et de protection des données. D'après le rapport « **Global Cybersecurity Outlook 2022** » du Forum économique mondial, une violation de cybersécurité coûte en moyenne 3,6 millions de dollars par incident. Les entreprises doivent se tenir prêtes.

« Les attaques sont imprévisibles, et il n'y a pas de signes avant-coureurs », insiste Dave Russell. « La direction doit s'en préoccuper, car la bonne gestion et la disponibilité appropriée des données deviennent un élément de plus en plus central des pratiques de sécurité. »

Les attaques ne constituent pas la seule menace. Au cours des trois dernières années, une entreprise sur cinq a subi des pannes importantes. C'est ce qu'indique le rapport « **2022 Annual Outage Analysis** »de l'Uptime Institute : « les problèmes de mise en réseau ont été à l'origine de la plupart des temps d'arrêt informatiques, quel que soit leur degré de gravité. »

Les sauvegardes et la redondance sont des précautions essentielles pour garantir la disponibilité des données, et c'est d'ailleurs souvent pour cette raison précise que les entreprises se tournent vers les environnements de cloud hybride. Si beaucoup de services cloud offrent des outils de redondance, les entreprises ne peuvent pas se permettre de confier la protection et la sécurité de leurs données au seul fournisseur de services.

« Les systèmes de gestion centralisée facilitent la mise en œuvre de solides mesures de sécurité techniques, telles que le chiffrement, l'automatisation, le contrôle d'accès, l'orchestration et la sécurité des terminaux. »

Kateryna Dubrova, analyste chez ABI Research

« L'innovation est possible à chaque instant »

Au moment du rachat de CA Technologies en 2018, puis de Symantec en 2019, Andy Nallappan, directeur technique et responsable de l'exploitation des activités logicielles chez Broadcom, savait qu'il fallait prévoir des changements majeurs dans l'environnement IT.

En effet, chaque entreprise composait avec diverses piles technologiques et opérations IT, via des ressources sur site, en colocation et dans le cloud. Broadcom souhaitait standardiser l'ensemble au sein d'une pile technologique moderne, tout en restant en phase avec la clientèle et se préparant aux changements à venir.

« Cela s'est avéré plus compliqué qu'une simple migration vers le cloud. Notre démarche de modernisation devait mettre à profit l'architecture cloud et en justifier le coût », précise Andy Nallappan.

Cet effort a fait intervenir plus de 20 partenaires, nécessité un vaste changement culturel et soulevé des questions quant à la conformité internationale, à l'intégration d'un spectre d'exigences de sécurité et aux besoins logiciels des workloads évoluant chaque jour, semaine et mois. Broadcom devait mener un travail de modernisation, de standardisation, de sécurisation et de déploiement à grande échelle.

À l'entame de l'année 2020, Andy Nallappan pensait que Broadcom pourrait parer aux bouleversements du marché. Sa nouvelle solution de cloud hybride, avec services locaux, de cloud public et de cloud privé intégrés et orchestrés, offrait une très grande flexibilité et agilité. La pandémie de Covid-19 n'a pas tardé à mettre à l'épreuve la solution de Broadcom. « De nombreux clients ont été contraints de migrer immédiatement vers le cloud », raconte Andy Nallappan. « Si nous n'avions pas réalisé ces changements à la suite de nos acquisitions, nous n'aurions pas pu nous adapter. »

« Avant la Covid, nous comptions quelque 750 000 utilisateurs. Après la Covid, ce chiffre a grimpé à 4 millions en quelques semaines », précise-t-il.

Andy Nallappan appelle à prendre conscience de l'intérêt du cloud. « Il n'est pas possible de tirer les meilleurs résultats si vous confiez la gestion à quelqu'un d'autre. C'est différent d'une solution sur site qui n'est pas propice à l'innovation. L'achat de la technologie donne l'impression d'un statu quo qui va durer cinq ans. Avec le cloud, en revanche, rien n'est figé. On peut apporter des changements tous les jours et l'innovation est possible à chaque instant. Ce pouvoir est entre nos mains », conclut-il.

Les sauvegardes constituent un aspect essentiel des plans de DR. « Prenons l'exemple d'une attaque par ransomware : que faire si vous perdez tout ? Si vos données sont compromises, vous devez être en mesure d'effectuer une restauration en remontant à un stade où leur intégrité ne fait aucun doute, et c'est précisément là que les sauvegardes entrent en jeu », ajoute Dave Russell.

Centralisation en faveur de la cohérence opérationnelle

Le cloud hybride requiert idéalement une plateforme de gestion cloud centralisée. Il est intéressant de centraliser et d'unifier les outils et les processus pour bénéficier d'un environnement convivial dans lequel les équipes peuvent travailler et collaborer en toute fluidité sur l'ensemble des instances locales et cloud (privé/public).

En plus de créer un écosystème propice à la collaboration interservice et à la cohérence opérationnelle, une telle centralisation améliore les performances de développement, ce qui contribue à raccourcir les délais de commercialisation. Selon le **rapport Cisco sur les tendances mondiales du cloud hybride en 2022**, 41 % des décideurs IT interrogés considèrent la collaboration comme un gage d'efficacité opérationnelle, tandis que 39 % d'entre eux affirment qu'elle améliore la performance des applications.

En outre, la cohérence opérationnelle assure la continuité de l'activité et renforce la sécurité. « Les systèmes de gestion centralisée facilitent la mise en œuvre de solides mesures de sécurité techniques, telles que le chiffrement, l'automatisation, le contrôle d'accès, l'orchestration et la sécurité des terminaux », explique Kateryna Dubrova. « Il est normal que les entreprises optent davantage pour des plateformes holistiques leur permettant d'équilibrer les workloads et de maintenir la continuité de l'activité à l'échelle de l'architecture IT hybride. »

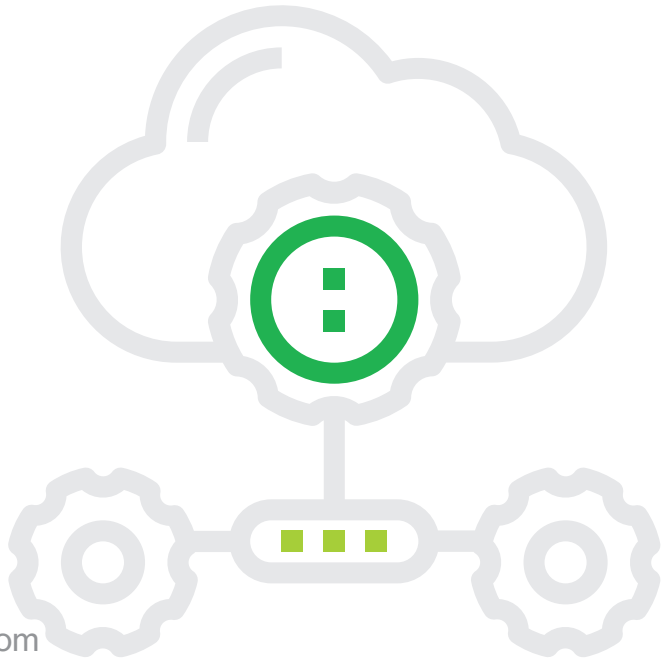
Cloud hybride et innovation

Le cloud hybride est bien parti pour s'imposer de facto comme LE modèle économique des entreprises. Toujours dans le cadre du rapport Cisco sur les tendances mondiales du cloud hybride en 2022, 82 % des répondants ont déclaré que leur entreprise avait adopté un modèle de cloud hybride. Ce fonctionnement permet d'adapter plus facilement les ressources système et ainsi de monter ou de descendre en puissance au gré des pics de demande à court terme, tout en offrant la disponibilité des données et la flexibilité nécessaires pour répondre aux besoins d'expansion et d'expérimentation.

Le cloud hybride simplifie également la complexité croissante des applications et soutient l'innovation. « On attend du cloud hybride qu'il mette les données à disposition immédiate pour la prestation de services », affirme Dave Russell. « La migration vers le cloud des workloads de production, en particulier, renforce les attentes liées à la disponibilité. »

Les entreprises qui adoptent des stratégies holistiques de protection des données sont ensuite en mesure de s'adapter à l'évolution constante des besoins, dans et en dehors du cloud. Au fil des avancées dans le domaine des technologies intelligentes et des produits autonomes et compte tenu de la généralisation progressive de l'informatique en périphérie, le cloud hybride va devenir un outil indispensable à la compétitivité des entreprises.

« Vous devez vous préparer maintenant — l'offre est déjà en place », conclut Dave Russell. « Il est temps de se pencher sur le cloud hybride, car le multicloud devient de plus en plus une réalité incontournable. »



« L'achat de la technologie donne l'impression d'un statu quo qui va durer cinq ans. Avec le cloud, en revanche, rien n'est figé. On peut apporter des changements tous les jours et l'innovation est possible à chaque instant. Ce pouvoir est entre nos mains. »

Andy Nallappan, directeur technique chez Broadcom

« Le succès du cloud hybride repose sur la protection des données » est un rapport de synthèse rédigé par MIT Technology Review Insights. Nous tenons à remercier toutes les personnes qui ont apporté leur concours à son élaboration, ainsi que le commanditaire, Veeam. MIT Technology Review Insights a agi en toute indépendance à l'heure de recueillir les informations et de formuler l'ensemble des constatations figurant dans ce document, sans égard à la participation ou au parrainage d'un quelconque tiers. Le présent rapport a été révisé par Laurel Ruma et Michelle Brosnahan, et édité par Nicola Crepaldi.

À propos de MIT Technology Review Insights

MIT Technology Review Insights est la division des services d'édition sur mesure du MIT Technology Review, le magazine technologique le plus ancien au monde qui reçoit le soutien du MIT, l'institut technologique de référence sur la scène internationale — organisant des événements en direct et produisant des recherches sur les technologies de pointe et les défis métier du moment. Insights mène des études et des analyses qualitatives et quantitatives aux États-Unis et dans d'autres pays, et publie un vaste éventail de contenus : articles, rapports, infographies, vidéos, podcasts, etc. Et par l'intermédiaire du MIT Technology Review Global Insights Panel, dont les effectifs ne cessent de croître, la division Insights est en posture idéale pour réaliser des sondages et des entrevues approfondies auprès des équipes de haute direction, innovateurs et entrepreneurs du monde entier.

À propos du commanditaire

Veeam® est le leader des solutions de sauvegarde, de restauration et de gestion des données qui assurent une protection moderne des données. La société propose une plateforme unique pour les environnements cloud, virtuels, physiques, SaaS et Kubernetes. Ses clients lui font confiance : ils savent que leurs applications et leurs données sont protégées et disponibles en permanence grâce à la plateforme la plus simple, la plus flexible, la plus fiable et la plus puissante du marché. Veeam protège plus de 400 000 clients dans le monde, dont 82 % des sociétés du Fortune 500 et 69 % de celles du Global 2000. L'écosystème mondial de Veeam compte plus de 35 000 partenaires technologiques, revendeurs, fournisseurs de services et partenaires Alliance, et la société possède des bureaux dans plus de 30 pays. Pour en savoir plus, consultez le site **www.veeam.com/fr** ou suivez **@veeam-software** sur LinkedIn et **@veeam** sur Twitter.

Illustrations
Illustrations sur la page de garde et dans le corps du rapport créées par Chandra Tallman Design LLC. Compilation à partir de The Noun Project.

MIT Technology Review Insights

www.technologyreview.com

@techreview @mittr_insights

insights@technologyreview.com