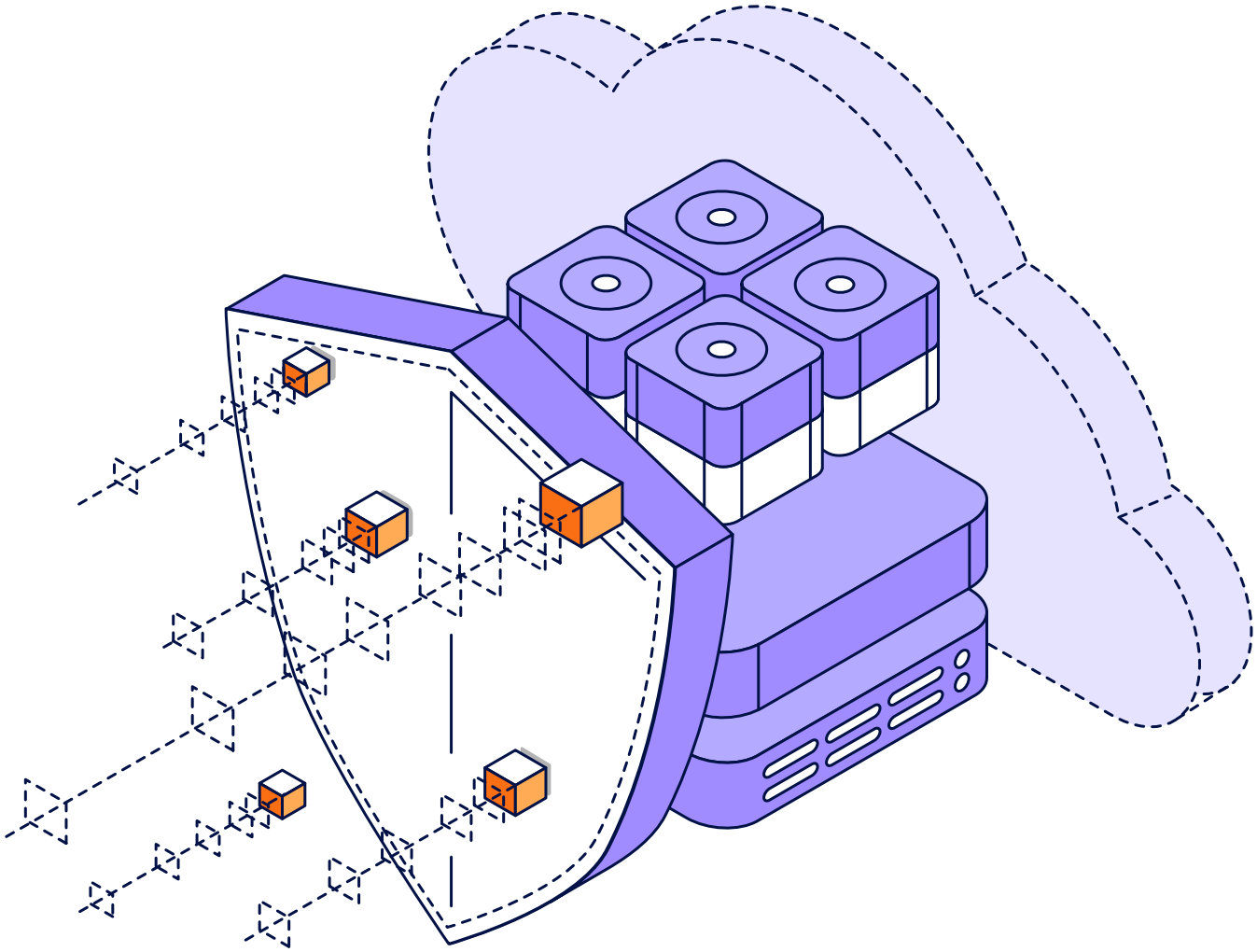
RAPPORT DE SYNTHÈSE

Les tendances de la protection du cloud en 2023

Édition EMEA



Durant l'automne 2022, un cabinet de recherche indépendant a mené une étude objective auprès de **1 700** responsables informatiques afin de déterminer l'utilisation qu'ils font des services cloud, aussi bien en production qu'à des fins de protection. Des profils représentatifs ont été interrogés pour chaque scénario, afin de cerner les différences entre leurs points de vue, ainsi que leurs motivations stratégiques et leurs méthodes de sauvegarde. Sur les **1 700** personnes interrogées, **650** résidaient dans la région EMEA.

Cette vaste étude de marché s'est intéressée à des entreprises impartiales exécutant au moins un workload de production dans un cloud (IaaS, PaaS ou SaaS). Elle a été réalisée pour le compte de Veeam afin de comprendre les perspectives et les responsabilités de différents profils, les méthodes à l'œuvre dans l'exécution et la protection des workloads hébergés dans le cloud, ainsi que les éléments pris en compte lors de l'utilisation d'une solution de protection des données cloud. Le rapport complet est disponible à l'adresse **http://vee.am/CPT23**.

IT hybride = mouvement fluide vers ET depuis les hôtes cloud

Pour la plupart des entreprises dotées d'une stratégie « cloud-first », les nouveaux workloads pouvant être exécutés dans un cloud sont mis en œuvre dans cet environnement, avec un peu moins d'**un tiers** des serveurs cloud lancés directement dans un hôte cloud et **deux tiers** ayant été migrés depuis le datacenter. Cela dit, le « parcours vers le cloud » n'est pas à sens unique, puisque la plupart des entreprises ont déjà rapatrié des workloads depuis le cloud.

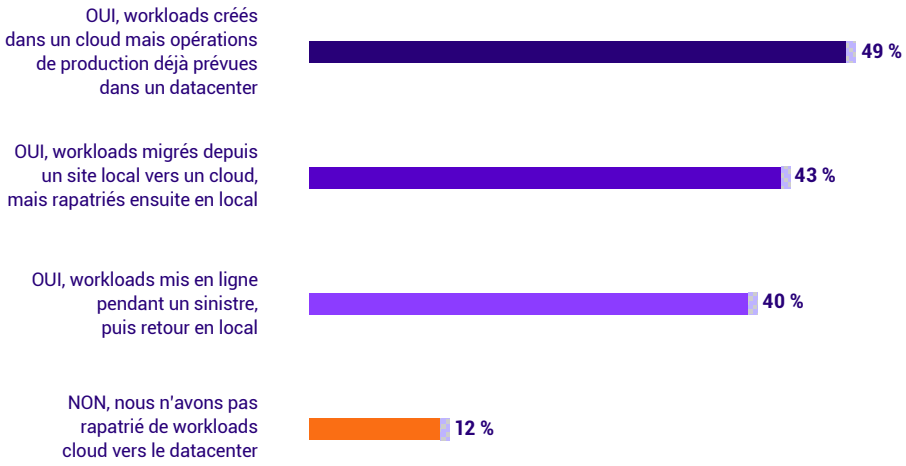


Figure 1.2

Votre entreprise a-t-elle RAPATRIÉ des workloads d'un cloud public vers un site local ?

Il convient de souligner que la fluidité des retours de workloads vers un site local varie quelque peu selon les régions :

	MONDE	Amériques	EMEA	APAC
NON, nous n'avons pas rapatrié de workloads cloud vers un site local	12 %	1 %	**26 %**	9 %
OUI (une ou plusieurs raisons)	88 %	99 %	**74 %**	91 %
OUI, dans le cadre d'une reprise après incident	40 %	45 %	**31 %**	45 %
OUI, workloads migrés depuis un site local, puis rapatriés depuis le cloud	43 %	46 %	**35 %**	51 %
OUI, workloads créés dans un cloud, exécution prévue dans un datacenter	49 %	52 %	**40 %**	59 %

74 %

des entreprises ont rapatrié des workloads vers leurs datacenters pour l'une des raisons suivantes : basculement dans le cadre d'une reprise après incident, phase de préparation / phase de production ou caractère inadéquat du cloud pour un workload.

Les emplacements d'origine des workloads hébergés dans le cloud sont très variés, tout comme les raisons pour lesquelles ces derniers sont rapatriés en local. C'est pourquoi, en 2023, les stratégies de protection des données devraient non seulement couvrir les workloads une fois qu'ils ont été migrés vers un cloud, mais également faciliter la migration depuis le cloud vers un datacenter, ou d'un cloud à un autre, selon les besoins de l'entreprise.

Bases de données et partages de fichiers cloud

Les infrastructures cloud offrent différentes possibilités de **partage de fichiers**, notamment :

- **76 %** exécutent des partages de fichiers dans des instances de serveurs hébergés (par ex., partages Windows Server ou Cloud ONTAP) ;
- **56 %** exécutent des services de partage de fichiers (SMB ou NFS) directement depuis un cloud à très grande échelle.

Affichant une dynamique similaire à celle des partages de fichiers cloud en tant que moyen privilégié de transférer des « données non structurées » vers des services cloud, les « données structurées » **(bases de données)** ont un taux d'adoption comparable :

- **78 %** exécutent des bases de données dans des instances de serveurs hébergés (par ex., serveurs Windows ou Linux) ;
- **56 %** exécutent des services de bases de données gérés directement depuis le cloud à très grande échelle.

L'exécution de services fondamentaux tels que les partages de fichiers et les bases de données revêt un intérêt « universel » pour les départements IT de toutes tailles, mais le recours à ces services cloud varie quelque peu, sans doute selon l'accessibilité à la bande passante et l'infrastructure cloud.

	MONDE	Amériques	EMEA	APAC
Partages de fichiers dans des instances de serveurs	76 %	86 %	67 %	75 %
Partages de fichiers via des services gérés	56 %	59 %	48 %	62 %
Bases de données dans des instances de serveurs	78 %	85 %	71 %	76 %
Bases de données via des services gérés	65 %	74 %	53 %	68 %

De fait, **91 %** des entreprises internationales interrogées exécutent des services de partage de fichiers et/ou bases de données d'un ou de plusieurs fournisseurs cloud. Ainsi, bien que les instances de serveurs « lift and shift » demeurent majoritaires, la diversité observée suggère qu'à partir de 2023, les stratégies de protection des données pour les environnements hébergés dans le cloud DEVRONT couvrir les partages de fichiers et bases de données désormais exécutés à partir de services cloud. Il est surprenant de constater que certaines entreprises sous-estiment l'importance des versions précédentes et de la rétention à long terme des données hébergées dans le cloud, quand les services PaaS sont nativement durables. En fait, la résilience des services cloud peut parfois pousser les entreprises, à tort, à ne pas sauvegarder leurs workloads cloud :

- **34 %** pensent que leurs **partages de fichiers** dans le cloud sont durables ou n'ont pas besoin d'être sauvegardés ;
- **15 %** pensent que leurs **bases de données** dans le cloud sont durables ou n'ont pas besoin d'être sauvegardées.

C'est une erreur.

91 %

des entreprises exécutent des partages de fichiers de production et/ou bases de données depuis un cloud, utilisant différentes combinaisons d'instances de serveurs et de services gérés.

À mesure que les offres gagnent en maturité et que les entreprises se sentent plus à l'aise, il est probable que la part des instances de serveurs diminue progressivement au profit des services gérés.

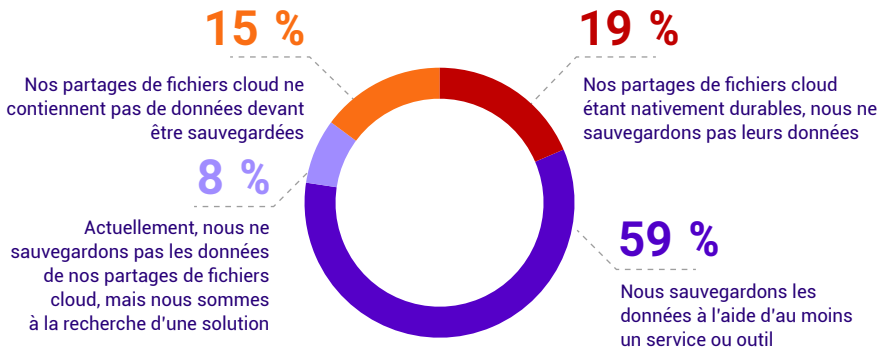


Figure 2.5

Comment sauvegardez-vous les données de vos partages de fichiers dans Amazon ou Azure ?

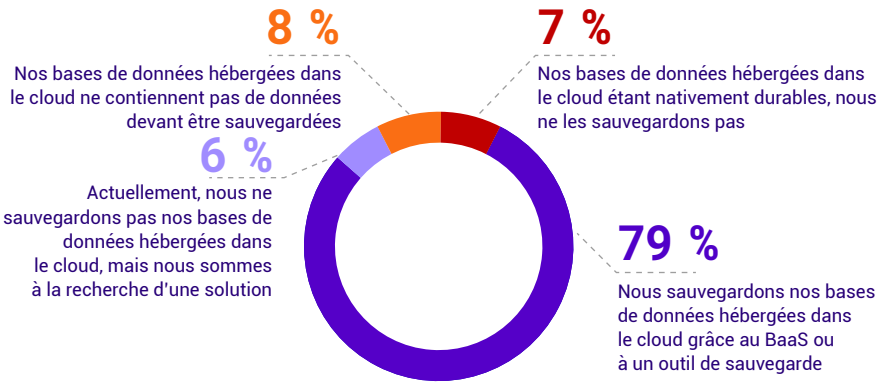


Figure 2.6

Comment sauvegardez-vous vos bases de données exécutées dans Amazon ou Azure ?

La multiplication des équipes modifie la stratégie de protection des données, mais une sauvegarde reste une sauvegarde

Aujourd'hui, de plus en plus de personnes sont impliquées dans les environnements cloud, notamment des spécialistes cloud et des propriétaires d'applications, encore plus que l'année précédente.

Une fois la stratégie établie, la plupart des sauvegardes des workloads cloud sont effectuées par l'équipe également en charge de sauvegarder les workloads de datacenter, aux deux tiers pour les administrateurs de sauvegarde **(69 %)** et le tiers restant pour les administrateurs de cloud **(31 %)**.

Dans les entreprises qui utilisent la sauvegarde en mode service (BaaS) pour leurs workloads hébergés dans le cloud, les membres de l'équipe BaaS s'occupent des tâches de sauvegarde un quart du temps, les équipes de sauvegarde et de cloud conservant proportionnellement un ratio de **deux tiers / un tiers** pour les tâches auto-gérées.

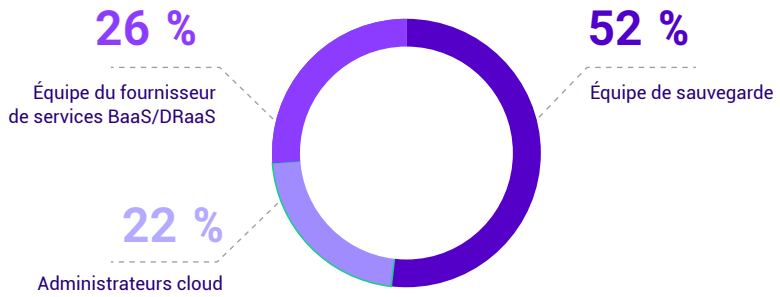


Figure 1.4

En règle générale, qui gère les sauvegardes/la protection des données des serveurs cloud dans votre entreprise ?

Briser les mythes de la sauvegarde de services M365

Il existe deux idées reçues courantes concernant SaaS et la protection des données :

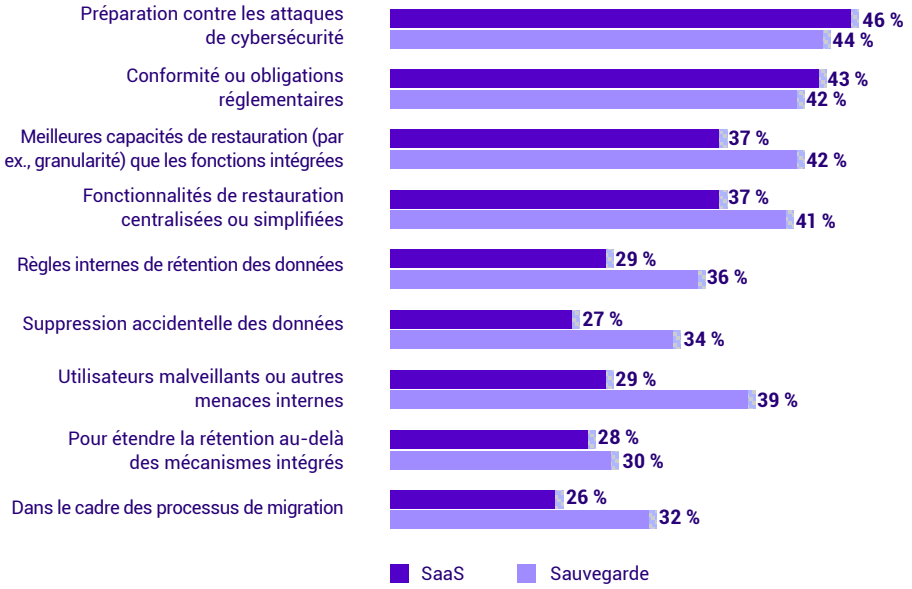
- La corbeille / les fonctionnalités d'annulation / de conservation intégrées sont suffisantes pour la sauvegarde.
- Les administrateurs d'applications ne comprennent pas l'importance des sauvegardes.

Ces deux hypothèses sont fausses. Au début d'un parcours de production « en mode service », de nombreuses entreprises pensent à tort que la résilience du serveur ou les fonctions d'annulation intégrées rendent la sauvegarde superflue. Cette confusion était surtout vraie au moment du lancement de M365, et les fonctionnalités avancées, telles que la « conservation légale », proposées dans les offres premium l'ont accentuée. Aujourd'hui, seules **4 %** des entreprises utilisent uniquement la corbeille M365 ou des fonctionnalités d'annulation similaires, et seulement **3 %** pensent à tort que la résilience de M365 rend la sauvegarde superflue. Quant aux **93 %** d'entreprises restantes utilisant M365 :

- **43 %** de celles qui utilisent les fonctionnalités avancées de M365 comprennent que celles-ci sont conçues pour des scénarios autres que la sauvegarde ou la rétention à long terme.
- Plus des trois quarts **(78 %)** utilisent un produit de sauvegarde tiers ou une solution BaaS pour sauvegarder leurs données M365.

Il convient de noter que le stockage Azure est la principale cible pour les données M365 à long terme. Utilisée par **42 %** des entreprises, cette solution permet d'excellentes restaurations si des informations d'identification distinctes sont utilisées pour limiter les cyber-risques.

Un autre malentendu entre les propriétaires d'applications et les administrateurs de sauvegarde porte sur les innombrables raisons de protéger les données. Alors que les propriétaires d'applications s'inquiètent principalement des temps de fonctionnement et du rollback, relativement récent, les administrateurs de sauvegarde ont tendance à se préoccuper davantage des obligations de conformité, des cyberattaques et autres incidents. Le tableau ci-dessous est plutôt rassurant, puisqu'il montre que les administrateurs M365 et les spécialistes de la sauvegarde sont globalement d'accord sur les principales raisons de sauvegarder les données M365.



Il n'y a pas si longtemps, la corbeille intégrée était « suffisante » pour la majorité des entreprises qui n'avaient pas encore compris la nécessité d'effectuer de véritables sauvegardes des données M365.

En 2021, **47 %** utilisaient uniquement la corbeille, contre **4 %** aujourd'hui. Par ailleurs, **78 %** utilisent désormais une solution de sauvegarde tierce, contre **45 %** en 2021.

Figure 3.4

Quelles sont les principales raisons de votre entreprise de protéger ses données Microsoft 365 ?

Pourquoi le BaaS ou le DRaaS ?

S'agissant des services de protection des données dans le cloud, il est important de connaître ces deux solutions :

- la sauvegarde en mode service (BaaS), axée sur la protection et la restauration des données via une cible et un service cloud ;
- la reprise après incident en mode service (DRaaS), axée sur la reprise d'activité à l'aide d'une infrastructure cloud plutôt qu'un basculement sur un site secondaire.

Quel que soit le service cloud, il convient tout d'abord de se poser cette question fondamentale : *« Quels sont les avantages du BaaS ou du DRaaS par rapport à la gestion de ma propre solution ? »*

- **Pour le BaaS,** la réponse est l'*efficacité opérationnelle.* Outre la survie et l'agilité des données (la capacité à accéder aux sauvegardes en tout lieu), les cinq raisons les plus courantes se résument à l'efficacité opérationnelle.
- **Pour le DRaaS,** les répondants ont cité une plus grande variété de raisons, les trois plus importantes portant sur l'*expertise* qu'un fournisseur DRaaS offre en complément aux équipes IT :
  - Expertise en matière d'implémentation
  - Expertise en matière de planification
  - Libération des experts IT en interne pour d'autres tâches

Ce n'est qu'après ces raisons relatives à l'expertise que viennent l'efficacité, l'amélioration des capacités et la supervision, c'est-à-dire les raisons qui justifient le BaaS. Autrement dit, si le BaaS peut être perçu comme une solution apportant des améliorations tactiques, le DRaaS se justifie par ses avantages stratégiques pour l'entreprise.

81 %

des entreprises prévoient d'utiliser une solution de protection des données cloud (BaaS ou DRaaS) d'ici 2023.

http://vee.am/DPR22

Le parcours vers la protection cloud

Aujourd'hui, **42 %** des entreprises utilisent le stockage cloud de la solution de sauvegarde de leur datacenter, tandis que **58 %** ont recours au BaaS. Mais ce n'est pas l'information la plus intéressante de cette illustration.

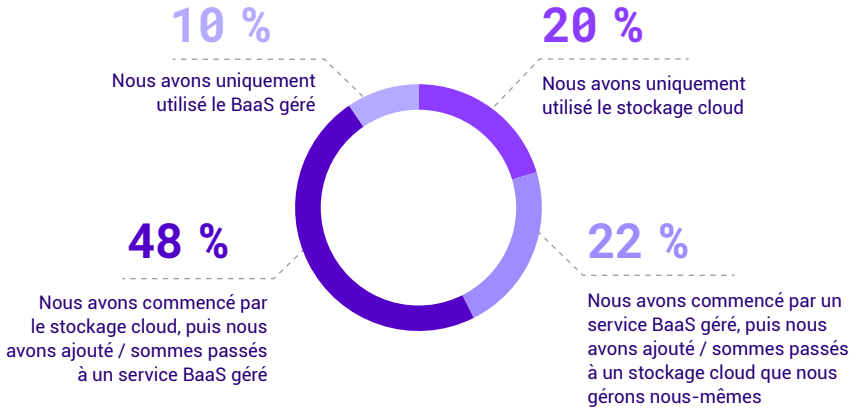


Figure 5.1

Comment décririez-vous l'utilisation des services/ stockage de sauvegarde cloud dans votre entreprise et son parcours ?

Parmi les grandes nouveautés du rapport sur les tendances de la protection du cloud de cette année, les personnes interrogées ont été invitées à préciser comment elles avaient commencé à ajouter des fonctionnalités cloud à leur stratégie de protection des données :

- Stockage cloud, dans le cadre d'une solution de protection des données traditionnelle
- Souscription d'un abonnement BaaS géré

Mais où en sont-elles aujourd'hui ?

- **30 %** n'ont rien changé.
- **70 %** sont passées d'une solution auto-gérée au BaaS ou inversement.

Parmi celles ayant changé de solution, près des deux tiers ont abandonné le stockage cloud au profit du BaaS (plutôt que l'inverse), ce qui signifie qu'elles sont nombreuses à avoir commencé avec des sauvegardes auto-gérées utilisant le stockage cloud (par ex., compartiment/blob à très grande échelle), mais qu'elles ont fini par profiter de la valeur ajoutée offerte par les fournisseurs de services : leur expertise. Alors que **22 %** ont commencé par le BaaS et ont décidé ensuite d'exécuter leurs propres cibles cloud, près de la moitié des personnes interrogées **(48 %)** ont utilisé un simple stockage cloud avant de se tourner vers le BaaS.

Il convient de souligner que ces statistiques varient selon les régions :

	Monde	Amériques	EMEA	APAC
Ont uniquement utilisé le stockage cloud	20 %	26 %	**15 %**	19 %
Ont commencé par le BaaS géré, puis sont passés au stockage cloud	22 %	38 %	**58 %**	47 %
Ont commencé par le stockage cloud, puis sont passés au BaaS géré	48 %	21 %	**20 %**	27 %
Ont uniquement utilisé le BaaS géré	10 %	14 %	**7 %**	7 %

S'agissant du type de cloud et de sa gestion, il n'y a pour ainsi dire pas de mauvaises réponses :

- Près de la moitié des entreprises **(46 %)** choisissent de gérer elles-mêmes leurs tâches de sauvegarde, mais font appel à un fournisseur BaaS pour la gestion des services/serveurs de sauvegarde. Ce seul point peut soulager considérablement les équipes IT grâce à la suppression des tâches de surveillance et de gestion des serveurs de sauvegarde, du stockage, des correctifs logiciels, etc.
- Un tiers des entreprises **(31 %)** préfèrent déléguer la plupart des opérations de sauvegarde (par ex., la supervision des tâches de sauvegarde, le capacity planning, les alertes et même les tâches de restauration) à des services d'assistance BaaS.

Encore une fois, il existe des différences selon les régions :

	Monde	Amériques	EMEA	APAC
Gestion IT principalement	46 %	45 %	**50 %**	41 %
Équilibre entre IT et FSS	23 %	18 %	**24 %**	28 %
Gestion FSS principalement	31 %	36 %	**26 %**	31 %

Le passage du stockage cloud au BaaS géré s'explique par l'intérêt croissant pour les services BaaS « clé en main » ou « haut de gamme ».

En 2021, seulement **13 %** des entreprises voulaient que leur fournisseur de services s'occupe de la majorité de la gestion, contre **31 %** aujourd'hui. Par ailleurs, **46 %** veulent gérer leurs propres services, contre **63 %** en 2021.

Le point de vue de Veeam

Plateforme de sauvegarde et de gestion des données de Veeam

Aujourd'hui plus que jamais, les établissements doivent avoir la certitude que leurs données sont protégées et disponibles en permanence, que ce soit en local, en périphérie ou dans le cloud. Veeam propose une plateforme unique pour les environnements cloud, virtuels, physiques, SaaS et Kubernetes. Nos clients nous font confiance : ils savent que leurs applications et leurs données sont protégées contre les ransomwares, les sinistres et les acteurs malveillants, et qu'elles sont toujours disponibles grâce à la plateforme la plus simple, la plus flexible, la plus fiable et la plus puissante du marché.

Veeam leur permet d'accélérer leur transformation numérique, de se protéger contre la cybercriminalité et de favoriser la résilience de leur activité, tout en garantissant la protection et la disponibilité de leurs données. Réduisez vos coûts, simplifiez les processus et atteignez vos objectifs avec Veeam, le nº 1 de la sauvegarde et de la restauration.

Pour en savoir plus, rendez-vous sur **https://www.veeam.com/fr**.

Cliquez ici pour consulter le rapport d'étude complet basé sur les données mondiales.

Toute question liée aux données et informations de cette étude peut être soumise à StrategicResearch@veeam.com.