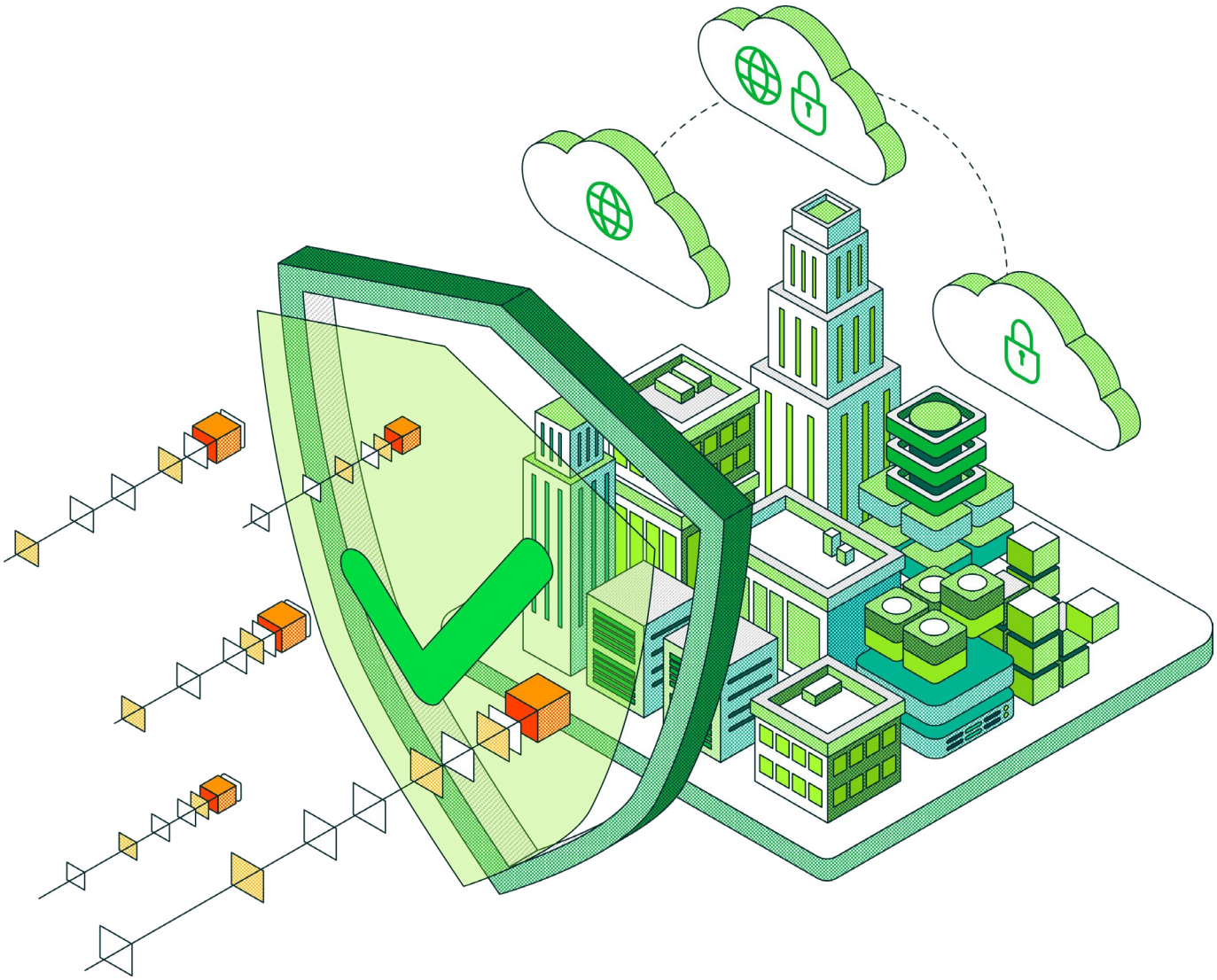
RAPPORT DE SYNTHÈSE

2023

Les tendances de la protection des données

Édition France



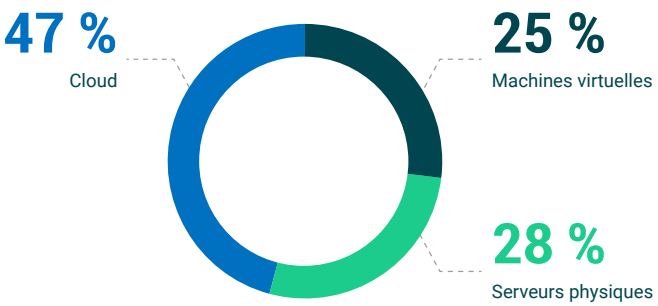
Fin 2022, un cabinet d'étude indépendant a interrogé de manière impartiale **4 200** décideurs et administrateurs IT, dont **395** en France, sur leurs motivations, problématiques et stratégies en matière de protection des données. Menée chaque année pour le compte de Veeam, cette vaste étude de marché impartiale lui permet d'aligner ses stratégies produits et ses initiatives commerciales sur l'évolution du marché de la protection des données.

Alors que Gartner prédit une augmentation des budgets IT globaux de **5,1 %** et qu'IDC prévoyait une augmentation des dépenses IT globales de **5,2 %**, cette enquête révèle que les budgets consacrés à la protection des données devraient augmenter de **6,5 %** dans le monde en 2023. Le rapport complet sur les tendances de la protection des données en 2023 est disponible à l'adresse https://vee.am/DPR23.

Infrastructure hybride de 2020 à 2025

Chaque année, l'enquête demande aux entreprises d'estimer leur proportion de serveurs sur site (physiques et virtuels) et hébergés dans le cloud pour l'année en cours, ainsi que leurs prévisions à deux ans. **Consultez le rapport complet** pour obtenir une synthèse des **12 000** réponses enregistrées sur les quatre enquêtes couvrant la période 2020-2025. Pour 2023, la répartition des instances de serveur dans les **4 200** entreprises dotées d'une infrastructure hybride est la suivante :

Paysage de l'informatique hybride en 2023 (au niveau mondial)



En 2023, les entreprises françaises envisagent d'augmenter leur budget consacré à la protection des données de

6,8 %

Dans l'ensemble, les serveurs **physiques** et les machines **virtuelles** s'équilibrent et représentent environ **50 %** de la stratégie IT globale d'une entreprise. Le reste est **hébergé dans le cloud**. On constate une évolution continue, bien que progressive, vers le cloud, principalement en raison d'une stratégie des entreprises qui donne la priorité au cloud en opérant un démarrage des nouveaux workloads dans le cloud à un rythme plus soutenu que la désactivation des anciens dans le datacenter. La part de ce dernier se trouve ainsi diluée au sein d'une stratégie IT hybride globale.

	MONDE	EMEA	All., Autr., Suisse	R-U, Irlande	**France**	Benelux	Italie	Esp., Port.	Scandinavie	Europe de l'Est	MEA
Serveurs physiques	28 %	28 %	29 %	28 %	**28 %**	28 %	29 %	29 %	28 %	27 %	29 %
Machines virtuelles	25 %	26 %	25 %	27 %	**25 %**	25 %	25 %	25 %	26 %	25 %	25 %
Cloud	47 %	46 %	46 %	45 %	**47 %**	47 %	46 %	46 %	47 %	48 %	46 %

L'essentiel à retenir : les solutions de protection moderne des données doivent offrir des fonctionnalités équitablement réparties sur les trois architectures (physique, virtuelle et cloud). En outre, il faut prévoir le déplacement des workloads entre les clouds et même leur retour sur site ; là encore, la stratégie de protection des données doit tenir compte de cette fluidité.

Que signifie « sauvegarde de niveau entreprise » ?

Pour la deuxième année consécutive, la caractéristique la plus importante d'une solution de sauvegarde de niveau entreprise est la **protection des workloads IaaS et SaaS.** Un constat peu surprenant si l'on considère la transition des infrastructures vers le cloud.

La deuxième caractéristique la plus importante est plus surprenante : la **fiabilité**. Sachant que de nombreuses entreprises exécutent des solutions de sauvegarde traditionnelles conçues pour l'ère du datacenter physique, il est fort probable que celles-ci utilisent des agents pour protéger les workloads cloud. Les processus de sauvegarde traditionnels offrent rarement de bons résultats lorsqu'il s'agit de protéger des workloads modernes.

Il est donc logique que la protection dans le cloud et la fiabilité soient prioritaires au même titre.

16 %

des entreprises françaises à la recherche d'une solution de sauvegarde de niveau entreprise considèrent prioritaire « **la protection des workloads IaaS et SaaS, et du datacenter** ».

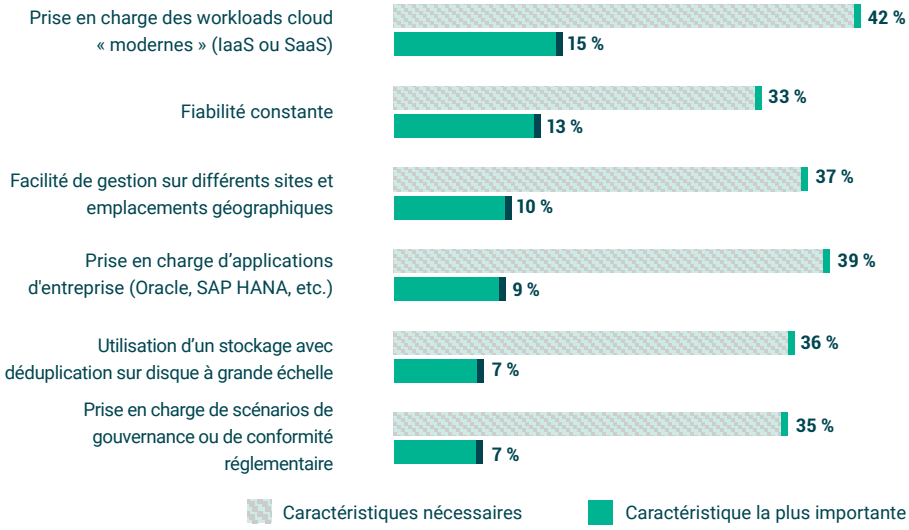


Figure 1.2

Pour vous, que signifie « sauvegarde de niveau entreprise » ?

Si votre entreprise devait envisager une nouvelle solution de « sauvegarde de niveau entreprise » aujourd'hui, quelle serait sa caractéristique la plus importante ?

En réalité, lorsque les entreprises sont interrogées sur les raisons de changer de solution de sauvegarde principale, elles citent le plus souvent et en priorité **l'amélioration de la fiabilité**, en toute cohérence avec ce qu'elles recherchent dans une solution de sauvegarde de niveau entreprise.

29 %

des entreprises françaises souhaitent changer de solution de sauvegarde pour « **améliorer la fiabilité/réussite des sauvegardes** ».

En 2023, la protection « moderne » des données est « cyber-résiliente »

La protection moderne des données a aussi son lot de défis à relever. Selon le rapport d'étude complet, pour la troisième année consécutive, les cyberattaques demeurent la principale cause des pannes les plus graves, avec des attaques par ransomware de plus en plus fréquentes :

- en 2021, **76 %** des entreprises ont subi au moins une attaque par ransomware ;
- en 2022, elles étaient **85 %**.

	MONDE	EMEA	All., Autr., Suisse	R-U, Irlande	**France**	Benelux	Italie	Esp., Port.	Scandinavie	Europe de l'Est	MEA
Aucune attaque en 2022	15 %	16 %	21 %	24 %	**18 %**	25 %	14 %	22 %	13 %	17 %	14 %
1 attaque seulement	18 %	19 %	24 %	19 %	**17 %**	24 %	17 %	21 %	23 %	23 %	18 %
2 ou 3 attaques	48 %	46 %	40 %	36 %	**49 %**	39 %	52 %	41 %	44 %	36 %	48 %
4 attaques ou plus	18 %	18 %	14 %	18 %	**15 %**	10 %	16 %	15 %	18 %	22 %	21 %

Des statistiques certes surprenantes, mais les résultats de ces attaques sont encore pires. Les entreprises ont été interrogées sur les attaques les plus importantes qu'elles aient subies en 2022 :

- **39 %** de leurs données de production ont été chiffrées ou détruites ;
- **55 %** seulement des données chiffrées/détruites ont pu être restaurées.

Sans surprise, l'aspect primordial le plus plébiscitéd'une solution moderne de protection des données repose sur l'intégration de celle-ci dans une stratégie de prévention des cybermenaces.

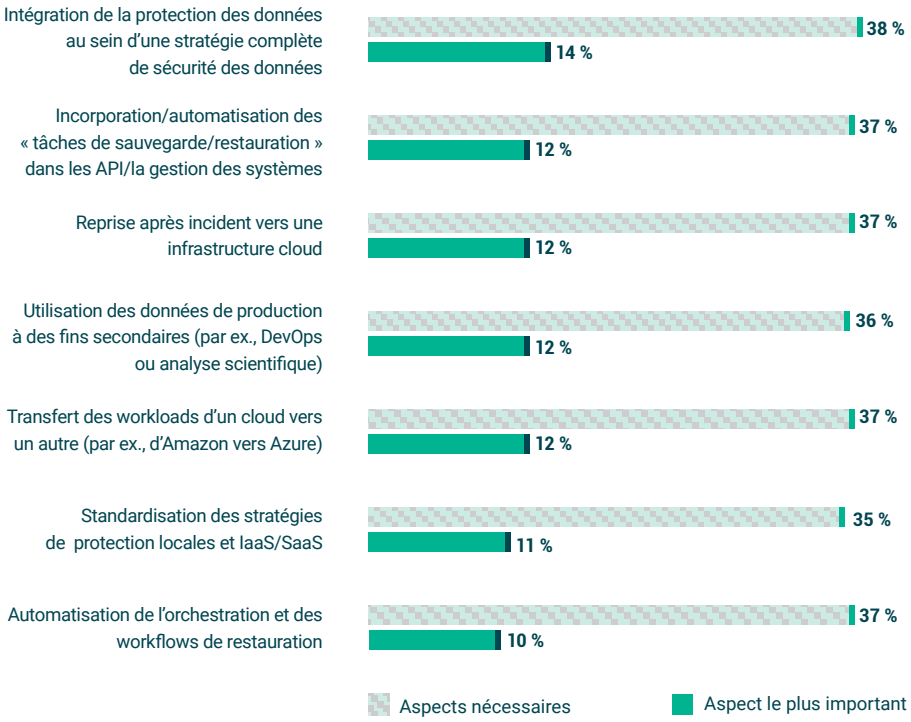


Figure 1.5

Quels sont les aspects d'une solution de protection des données « moderne » ou « innovante » pour votre entreprise ?
Et l'aspect le plus important ?

Mais si la cyber-résilience figure parmi les préoccupations majeures de nombreux responsables IT, concentrer toute une stratégie de protection des données sur les attaques constituerait une véritable erreur stratégique. Les pannes système, causées par des problèmes de réseau et de système d'exploitation ou des défaillances applicatives ou matérielles, restent monnaie courante, même au sein des datacenters modernes. Les entreprises doivent donc se préparer à affronter de telles complications, mais aussi des événements d'origine humaine, comme les erreurs d'utilisateurs et les attaques cybercriminelles.

BCDR : méthodes et procédés

Avec des services cloud de plus en plus couramment utilisés dans les stratégies de protection des données, de nombreuses entreprises se demandent s'il vaut mieux restaurer leurs données vers des serveurs sur site ou vers des infrastructures cloud. L'étude révèle un intérêt relativement égal pour les restaurations sur site et celles dans le cloud en 2023. Néanmoins, la plupart des données seront restaurées depuis des sauvegardes cloud. Cela s'inscrit dans la pratique qui consiste à limiter les points de restauration sur site et à transférer les données de l'entreprise vers un stockage cloud externe à des fins de rétention des données, de préparation à la BCDR et de prévention des ransomwares.

Si l'on part du principe que les principaux experts ne sont plus disponibles durant une crise, la plupart des planificateurs de BCDR recommandent fortement d'utiliser des workflows orchestrés grâce auxquels l'expertise est incluse dans les processus. Il est également recommandé de tester les workflows comme s'ils s'exécutaient pendant une véritable crise. Malheureusement, les résultats de cette année révèlent que seulement **18 %** des entreprises disposent de workflows orchestrés au sein de leur stratégie actuelle de protection des données ou de basculement.

53 %

des entreprises françaises envisagent d'utiliser des serveurs sur site pour leur BCDR, alors que **46 %** opteront pour une infrastructure dans le cloud.

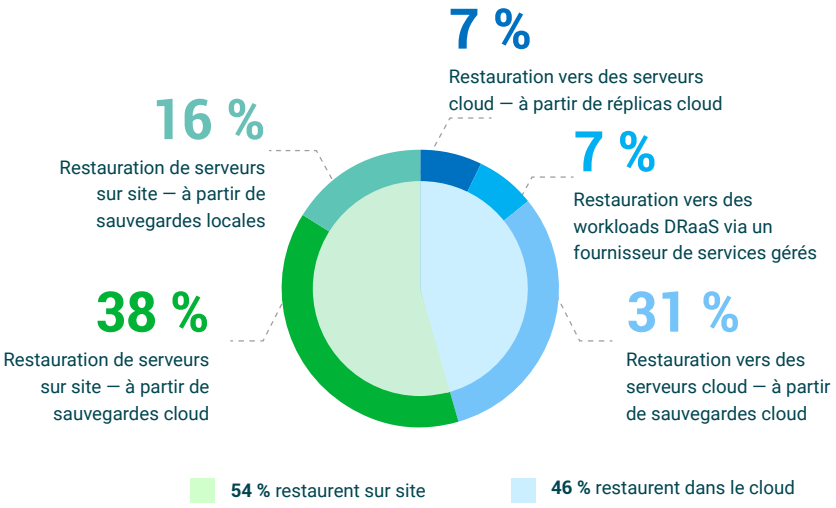


Figure 2.3

Comment rétablissez-vous l'exploitation dans le cadre de votre DR ?

La protection des données dans le cloud toujours très plébiscitée

Le stockage cloud signifie-t-il la fin des bandes ? Selon les résultats de l'étude, **50 %** des données sont toujours sauvegardées sur bande à un moment de leur cycle de vie, alors que **63 %**des données sont aujourd'hui stockées dans le cloud. Ces chiffres varient néanmoins en fonction des pays ou des régions.

	MONDE	EMEA	All., Autr., Suisse	R-U, Irlande	**France**	Benelux	Italie	Esp., Port.	Scandinavie	Europe de l'Est	MEA
% de données sauvegardées sur bande	50 %	53 %	48 %	42 %	**51 %**	53 %	51 %	49 %	52 %	53 %	52 %
% de données sauvegardées dans le cloud	63 %	63 %	63 %	56 %	**64 %**	65 %	66 %	63 %	63 %	69 %	64 %

Pour la rétention des données, de nombreuses entreprises utilisent un modèle opérationnel basé sur trois « tiers » :

- une sauvegarde sur disque local pendant 90 à 120 jours ;
- des copies dans le cloud, notamment des copies actuelles et des versions antérieures, pendant deux à cinq ans ;
- une sauvegarde sur bande pour une minorité de données qui doivent obligatoirement être stockées pendant 10 ans ou plus.

En guise d'alternative au « % de données utilisant le cloud », il convient de considérer « le % d'entreprises utilisant la sauvegarde cloud » : **67 %** des répondants au niveau mondial utilisent des services cloud dans le cadre de leur stratégie actuelle de protection des données, l'objectif étant d'atteindre **74 %** d'ici 2025.

Parmi les synergies les plus puissantes entre services cloud et protection des données, l'avènement de la reprise après incident dans le cloud permet de tirer parti des infrastructures cloud plutôt que ou en complément d'un datacenter secondaire. En 2020, **53 %** des entreprises disposaient d'une stratégie de BCDR ; elles sont **71 %** en 2023. Plus important encore, si environ **30 %** des entreprises continuent à tirer parti de plusieurs datacenters pour leur BCDR, le pourcentage de celles qui utilisent des services cloud (IaaS/DR ou DRaaS) pour leur BCDR a plus que doublé entre 2020 **(23 %)** et 2023 **(47 %)**, et elles sont **55 %** à envisager d'utiliser une DR dans le cloud d'ici 2025.

69 %

des entreprises françaises envisagent d'utiliser des services cloud dans le cadre de leur stratégie de protection des données d'ici 2025.

	MONDE	EMEA	All., Autr., Suisse	R-U, Irlande	**France**	Benelux	Italie	Esp., Port.	Scandinavie	Europe de l'Est	MEA
% d'entreprises utilisant une infrastructure cloud pour leur BCDR	47 %	41 %	49 %	41 %	**46 %**	47 %	40 %	52 %	54 %	49 %	41 %
% d'entreprises possédant plusieurs datacenters pour leur BCDR	24 %	25 %	23 %	34 %	**23 %**	22 %	26 %	23 %	24 %	24 %	25 %

2023, l'année du changement ?

Entre l'angoisse des ransomwares, la pression pour garantir les services IT et les défis de la protection des workloads IaaS et SaaS modernes, vous pouvez en conclure à raison que de nombreuses entreprises vont changer de solution de sauvegarde pour s'adapter à ces nouvelles pressions et conditions. En ignorant les **35 %** de réponses quasi neutres :

- **8 %** des entreprises seulement ne changeront probablement pas de solution de sauvegarde principale en 2023 ;
- à l'inverse, **57 %** des répondants changeront probablement ou définitivement de solution de sauvegarde.

52 %

des entreprises françaises envisagent de changer de solution de sauvegarde en 2023.

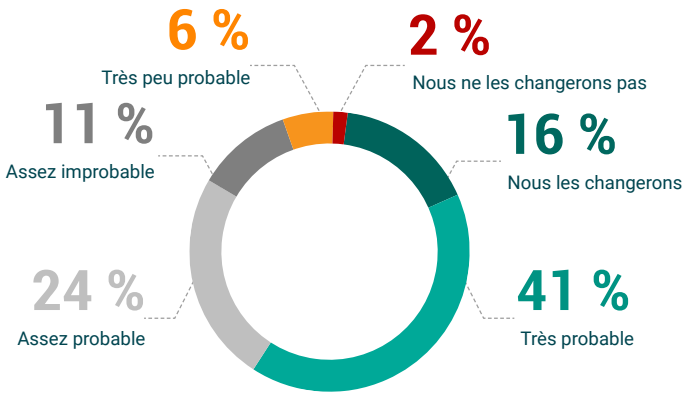


Figure 3.6

Quelle est la probabilité que votre entreprise change ses principaux services/solutions de sauvegarde dans les douze prochains mois ?

La perspective Veeam

La Veeam Data Platform

Alors que les entreprises poursuivent la transformation de leur infrastructure en assurant la prise en charge de la sauvegarde, l'utilisation et la mobilité cloud, une solution s'avère nécessaire pour démystifier les complexités. La Veeam® Platform offre les fonctionnalités suivantes :

- le contrôle des coûts du stockage à l'aide d'une architecture de tiering de stockage cloud intelligente ;
- la sauvegarde et la restauration, la reprise après incident et la mobilité Kubernetes natives conçues spécifiquement pour les applications conteneurisées ;
- une prise en charge étendue des workloads IaaS/PaaS/SaaS ;
- une supervision et une gestion centralisées, associées à une large couverture des API.

Les utilisateurs Veeam, qu'ils soient nouveaux ou existants, sont encouragés à découvrir les fonctionnalités phares de Veeam Backup *for AWS, Azure, Google Cloud, Microsoft 365, Salesforce,* et de Kasten for Kubernetes : elles sont spécifiquement conçues pour répondre aux besoins uniques du cloud hybride.

Les utilisateurs Veeam à la recherche de solutions « en mode service », ou qui souhaitent combler un manque de ressources, peuvent se tourner vers le réseau de partenaires Veeam, qui comprend de nombreux fournisseurs de BaaS et de DRaaS ainsi que des spécialistes des services professionnels, pour optimiser leurs investissements Veeam dans le cloud.

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 envoyée à l'adresse **StrategicResearch@veeam.com**.