



RAPPORT ESG RESEARCH INSIGHTS

Pourquoi la protection des données est-elle importante pour les environnements multi-Cloud actuels ?

Une étude explorant le rôle des fonctionnalités optimisées de protection des données pour un Cloud hybride réussi

Par Christophe Bertrand, Analyste senior

Mai 2020

Ce rapport Research Insight d'ESG a été commandé par Dell Technologies, VMware et Intel Corporation et est distribué sous licence par ESG.

Contenu

Les tendances, l'évolution et l'étalement du Cloud façonnent un paysage changeant en matière de protection des données	3
La protection des données : un facteur essentiel à la réussite du Cloud hybride	6
Les avantages d'une protection des données optimisée pour les environnements multi-Cloud.....	6
Ce qu'il faut retenir.....	9
Comment Dell Technologies peut vous aider	10
Annexe : méthodologie de recherche et caractéristiques démographiques des personnes interrogées	11

Les tendances, l'évolution et l'étalement du Cloud façonnent un paysage changeant en matière de protection des données

Aujourd'hui, le Cloud gagne en popularité et son adoption se généralise au sein des entreprises, refaçonant ainsi l'infrastructure traditionnelle. L'étude ESG a révélé que 76 % des entreprises accordent au Cloud public autant ou plus d'importance qu'à l'infrastructure sur site pour les nouvelles applications, ce qui témoigne d'une grande confiance. En fait, 38 % des données des entreprises devraient résider dans le Cloud d'ici à 24 mois, tandis que le nombre de Clouds publics en cours d'utilisation devrait également augmenter.

Les utilisateurs de fournisseurs de services Cloud (CSP) ne mettent pas tous leurs œufs dans le même panier : 82 % d'entre eux font actuellement appel à plusieurs CSP, tandis que 86 % d'entre eux s'attendent à faire de même dans les 3 prochaines années. Plus précisément, la proportion d'utilisateurs ayant recours à plus de trois CSP devrait doubler (31 % contre 15 %) dans le même laps de temps. Dans ce contexte, il n'est pas surprenant que 73 % des entreprises déclarent que l'utilisation d'une infrastructure dans le Cloud public (ou dans plusieurs Clouds publics), en plus d'une infrastructure sur site, complique les opérations IT. L'ère du multi-Cloud est arrivée, avec son lot de complexités !

Cela implique que de nombreux processus liés aux données, tels que la sauvegarde et la récupération, doivent s'adapter à cet environnement hybride (dans lequel certaines charges applicatives sont sur site et d'autres sont hébergées sur une infrastructure de type Cloud public) et multi-Cloud (dans lequel les charges applicatives sont hébergées sur un large éventail de Clouds publics) en constante évolution. La protection des données « suit » les charges applicatives, cette relation étant corroborée par les recherches d'ESG : les entreprises disposant d'un environnement de plus de 500 machines virtuelles hébergées dans le Cloud sont plus susceptibles, par rapport à celles ayant 500 machines virtuelles ou moins, d'utiliser à la fois la reprise après sinistre en tant que service (DRaaS, 80 % contre 57 %) et les cibles de sauvegarde Cloud (82 % contre 69 %).¹ En d'autres termes, la propension d'une entreprise à utiliser différentes solutions de protection augmente en même temps que l'utilisation de l'aaS.

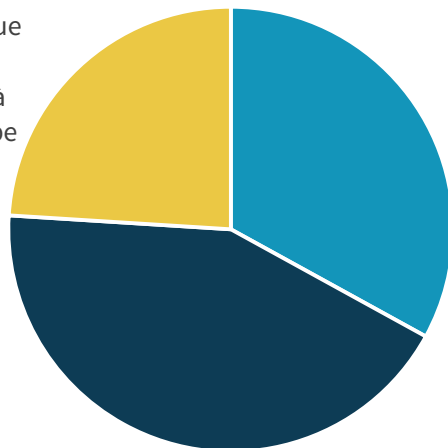
Il convient également de maintenir des objectifs cohérents en matière de point et de temps de récupération (RPO et RTO) au regard d'une infrastructure devenue très distribuée avec différents niveaux de contrôle, de sécurité et de gestion. Les implémentations en matière de protection des données doivent unifier les niveaux de service dans les environnements sur site et dans le Cloud. Il est donc possible de faire évoluer les conceptions architecturales actuelles de protection des données pour adopter des technologies capables de gérer les environnements de votre entreprise et de votre Cloud de manière cohérente.

¹ Source : ESG Master Survey Results, [Data Protection Cloud Strategies](#), juin 2019

Figure 1. Solution Cloud ou sur site : laquelle choisir en premier ?

Parmi les propositions suivantes, laquelle décrit le mieux l'approche adoptée par votre entreprise en matière de déploiement de nouvelles applications ? (Part de répondants, N = 1 257)

Politique de priorité à une infrastructure sur site, c'est-à-dire que nous déployons une nouvelle application à l'aide d'une infrastructure sur site, à moins que quelqu'un n'ait des arguments convaincants pour la déployer à l'aide d'une infrastructure de type Cloud public, 24%



Politique de priorité au Cloud public, c'est-à-dire que nous déployons une nouvelle application à l'aide d'une infrastructure de type Cloud public, à moins que quelqu'un n'ait des arguments convaincants pour la déployer en utilisant des ressources sur site, 33%

Nous prenons en compte à la fois les ressources technologiques sur site et les services de Cloud public lorsque nous réfléchissons au moyen de déploiement de nouvelles applications, 43%

Source : Enterprise Strategy Group

De nombreuses décisions relatives aux solutions de protection des données s'articuleront autour du point où les charges applicatives résident ; et les utilisateurs finaux privilégient la flexibilité du placement des charges applicatives : pour 83 % des entreprises, atteindre une flexibilité de placement des charges applicatives – ou la possibilité d'exécuter des charges applicatives sur le Cloud de leur choix, sur site ou à l'extérieur – figure parmi les 5 priorités absolues en matière d'initiatives technologiques. Cela signifie que les mécanismes de protection des données devront démontrer le même niveau de flexibilité pour répondre aux exigences de sauvegarde et de récupération et aux niveaux de service.

Bien que les environnements multi-Cloud suscitent de l'enthousiasme, les personnes interrogées **accordent généralement l'avantage fonctionnel aux environnements sur site**. Ce constat est particulièrement vrai concernant les fonctionnalités de sécurité et de facilité de gestion. Pour preuve, 77 % des entreprises interrogées ont rapatrié une charge applicative stratégique résidant dans le Cloud (en d'autres termes, une application ou un ensemble d'applications prioritaires dont l'entreprise dépend) pour diverses raisons techniques et opérationnelles.

Les exemples suivants ont été signalés par les entreprises qui avaient déployé des applications spécifiques dans le Cloud (ne concerne pas tous les utilisateurs interrogés dans le cadre de l'étude) :

- 27 % d'entre elles ont retiré des applications de gestion de la chaîne logistique.
- 25 % d'entre elles ont retiré des applications de gestion de la relation client.
- 24 % d'entre elles ont retiré des applications de planification de ressources d'entreprise.

Même parmi les charges applicatives émergentes, les pourcentages étaient largement cohérents :

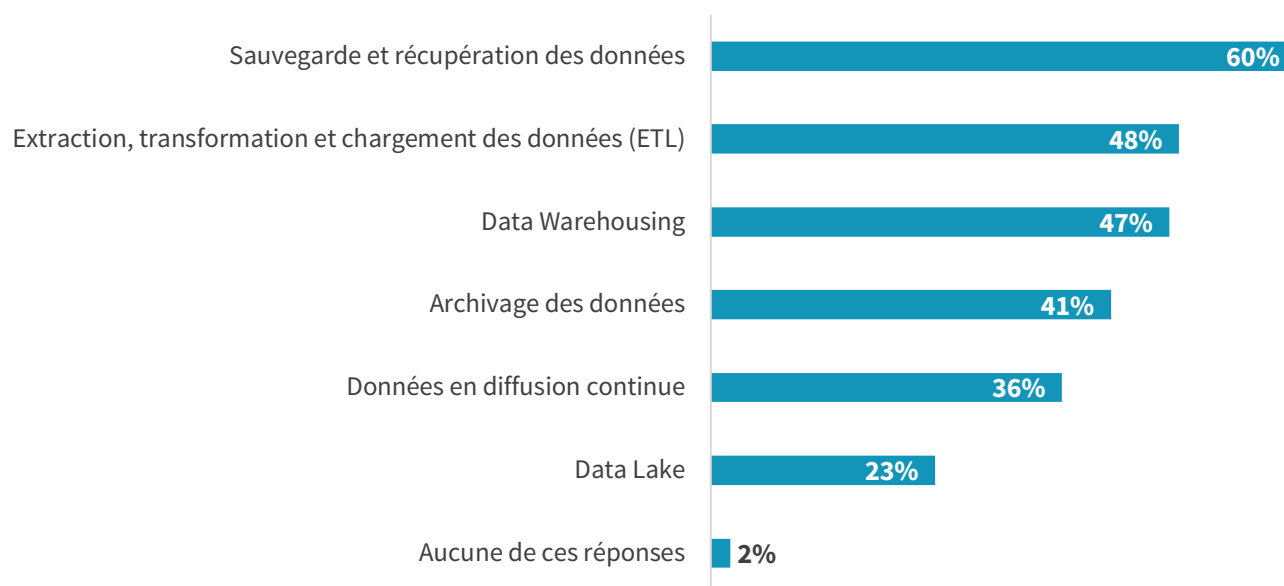
- 25 % d'entre elles ont retiré une charge applicative d'apprentissage automatique.
- 24 % d'entre elles ont retiré leurs environnements de Data Lake.
- 23 % d'entre elles ont retiré des charges applicatives d'analytique du Big Data.
- 21 % d'entre elles ont retiré des charges applicatives de Deep Learning.

Les principales raisons pour lesquelles les entreprises interrogées ont rapatrié leurs charges applicatives sont : la difficulté à mettre en œuvre des mesures de sécurité, des coûts excessifs ou imprévisibles, des problèmes liés à la technologie et à l'évolutivité, la sauvegarde et la récupération des données, et l'archivage. Quelle que soit la raison du rapatriement d'une application spécifique, comme indiqué précédemment, les processus de sauvegarde et de récupération « suivent » la charge applicative. Dans ce cas, il s'agit d'un retour sur site.

Les entreprises interrogées citent le plus souvent la protection des données comme étant l'une des charges applicatives de gestion des données les plus stratégiques pour leur organisation. De nombreuses parties prenantes internes s'attendent éventuellement à ce que la protection des données soit assurée automatiquement, ce qui, bien sûr, n'est pas le cas pour les nombreuses raisons que nous avons évoquées. Cependant, cela constitue une occasion pour les professionnels de l'IT et les parties prenantes de l'entreprise de discuter du rôle et des niveaux de service nécessaires à certaines fonctions ou applications métiers, ce qui permet ensuite de déterminer la solution optimale à déployer.

Figure 2. La sauvegarde et la récupération des données : des charges applicatives de gestion des données stratégiques prioritaires

Parmi les charges applicatives de gestion des données suivantes, laquelle classeriez-vous comme la plus stratégique au sein de votre entreprise ? (Part de répondants, N = 1 257, trois réponses acceptées)



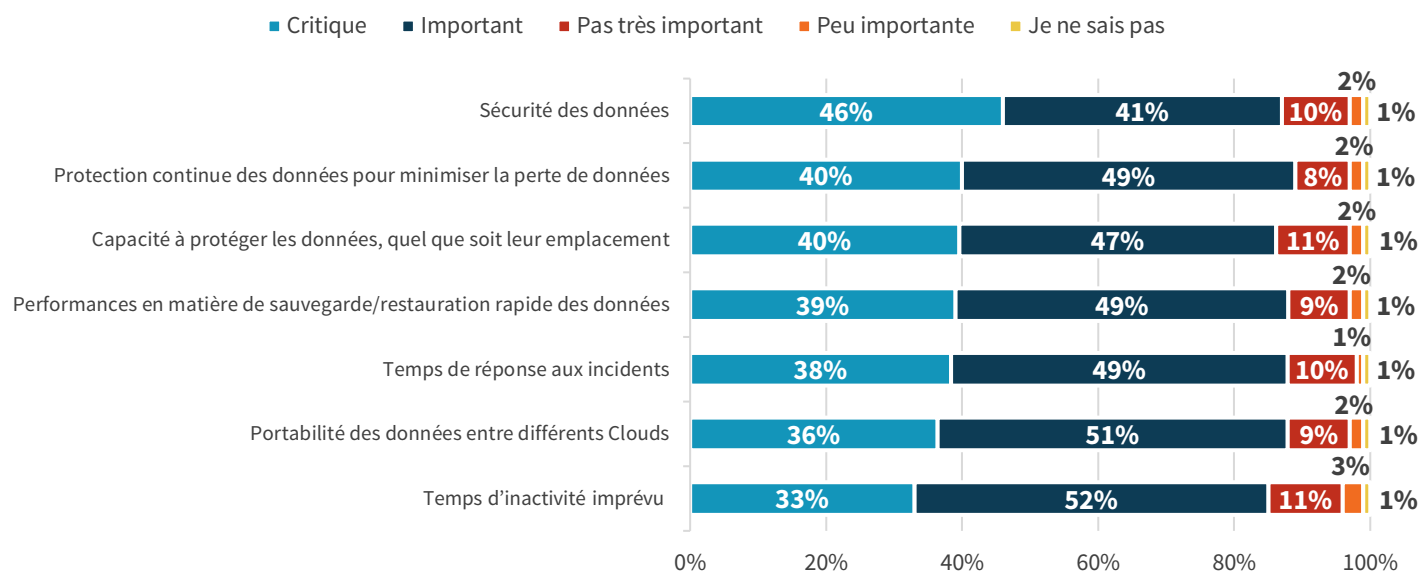
Source : Enterprise Strategy Group

La protection des données : un facteur essentiel à la réussite du Cloud hybride

Alors que 89 % des professionnels de l'IT estiment que la protection continue des données est essentielle à la réussite du Cloud hybride, 87 % d'entre eux ont le même sentiment vis-à-vis de la sécurité des données et de la capacité à protéger les données, quel que soit leur emplacement. Cela signifie que la solution qu'ils déploient doit offrir le type d'agilité et de fonctionnalité qui s'étend à plusieurs emplacements, sur site ou dans le Cloud, et des topologies capables de suivre les charges applicatives. Sans surprise, la sécurité des données est une préoccupation majeure pour les entreprises interrogées par ESG, tout comme la capacité à limiter la perte de données ou à atteindre de faibles RPO.

Figure 3. La protection des données sur site : un facteur important pour la réussite dans le Cloud hybride

Dans quelle mesure pensez-vous que chacune des caractéristiques suivantes relatives à l'environnement de protection des données sur site sont importantes pour parvenir à un environnement de Cloud hybride efficace ? (Part de répondants, N = 1 257)



Source : Enterprise Strategy Group

Les avantages d'une protection des données optimisée pour les environnements multi-Cloud

La protection des données a évolué au fil des années et a connu de nombreuses innovations et itérations technologiques. Bien que nous n'ayons pas l'intention de fournir une liste exhaustive dans ce document, ESG, en s'appuyant sur ses recherches et son expertise du domaine, définit généralement la protection des données « optimisée » comme une protection capable d'effectuer une sauvegarde et une récupération avancée et riche en fonctionnalités des données sur site et dans le Cloud (Cloud en tant que cible ou en tant que source), y compris des logiciels en tant que service. Cela inclut la capacité à protéger les environnements physiques et virtuels, ainsi que les applications exécutées sur l'infrastructure de conteneurs et l'optimisation de la consommation de stockage à l'aide de la déduplication. Les solutions de protection des données optimisées sont conçues pour être faciles à utiliser, mais offrent des fonctionnalités avancées de gestion et de création de rapports, et peuvent être exécutées en tant que services. La protection des données optimisée est en train d'évoluer vers une gestion intelligente des données.

En adoptant une perspective plus large sur le Cloud, les stratégies de Cloud efficaces peuvent être en partie définies comme étant dotées de puissantes fonctionnalités de Cloud hybride, comme la possibilité de choisir entre les technologies de Cloud public et de Cloud privé en fonction des besoins métiers et en matière de charge applicative, et non de facteurs externes arbitraires.

Dans un monde axé sur le Cloud, l'IT doit fournir des services plus rapidement, mais aussi à moindre coût. Les technologies de protection des données optimisée aident les départements IT à atteindre ces objectifs. Permettre aux entreprises de protéger les données où qu'elles se trouvent et en toute confiance leur donne la possibilité de déployer de nouveaux services Cloud (qu'ils soient sur site ou non) rapidement, tout en les assurant que les mécanismes de protection qui sous-tendent ces services les protègent. Pour preuve, lorsqu'ESG a demandé aux participants d'indiquer le pourcentage des projets Cloud terminés en retard, à la date prévue et en avance, les entreprises dotées d'environnements de protection des données optimisée ont déclaré avoir terminé 57 % de leurs projets en avance (33 % contre 21 %).

Les entreprises dotées d'environnements de protection des données optimisée ont signalé avoir réalisé plus de 57 % de leurs projets en avance

Les entreprises dotées d'environnements de protection des données optimisée ont signalé avoir augmenté de 59 % la part de projets réalisés en deçà de leur budget

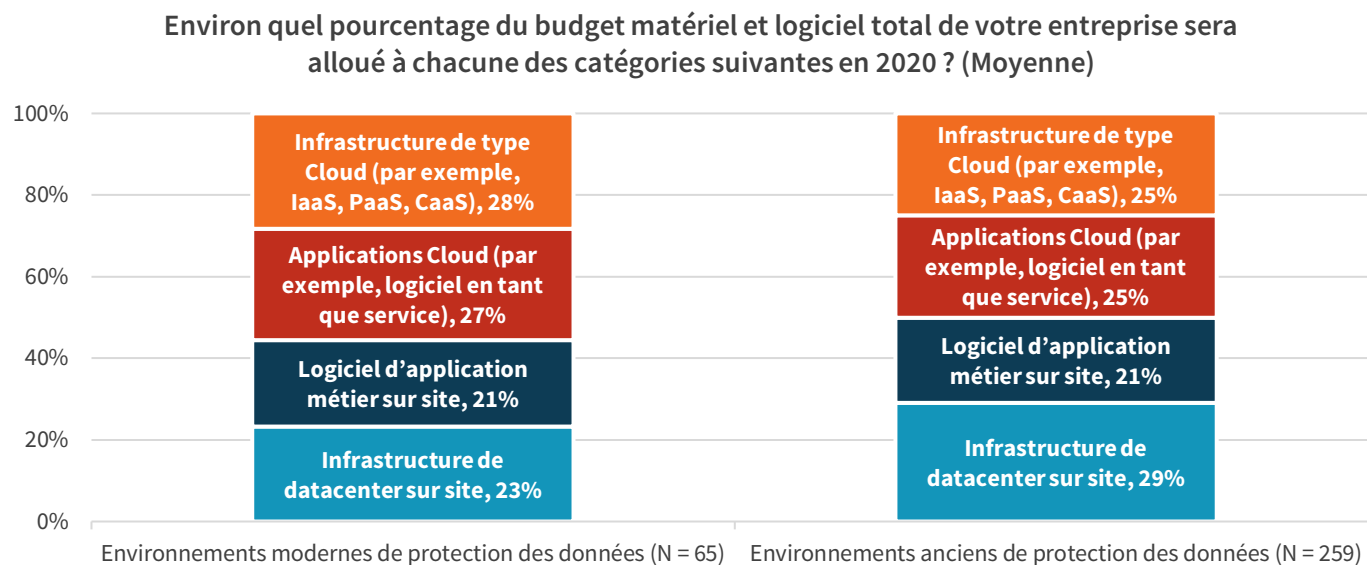
La main-d'œuvre est un élément important du coût d'un projet Cloud. Le temps des développeurs, des architectes IT, des architectes de la sécurité et des spécialistes de la protection des données est coûteux. Ainsi, réaliser des projets plus rapidement signifie également augmenter leur rentabilité. Lorsqu'ESG a demandé aux entreprises interrogées quel pourcentage des projets Cloud ont été réalisés en deçà du budget, conformément au budget ou ont dépassé le budget, celles qui disposent d'environnements

de protection des données optimisée ont déclaré avoir augmenté de 59 % la part de projets réalisés en deçà de leur budget (27 % contre 17 %).

Les investissements destinés à optimiser la protection des données semblent s'avérer rentables dans la mesure où ils réduisent les dépenses d'infrastructures sur site tournées vers l'avenir. Les « anciennes » installations de protection des données allouent 26 % de budget en plus à la modernisation de l'infrastructure sur site (29 % contre 23 %). D'après des recherches ESG antérieures, le budget IT annuel d'une entreprise moyenne est d'environ 167 millions de dollars USD.² La possibilité de réaffecter 6 % du budget IT (soit un peu plus de 10 millions de dollars USD pour une entreprise moyenne) à des projets plus stratégiques peut avoir un impact considérable.

En tant qu'utilisateur final, ces données indiquent que si vous disposez d'un environnement de protection des données robuste et optimisé, vous n'avez pas besoin de dépenser de l'argent pour sa mise à jour ou sa mise à niveau. La gestion de l'environnement prend également moins de temps. Tout cela explique pourquoi ces entreprises allouent 6 % de leur budget en moins à l'infrastructure sur site.

² Source : ESG Master Survey Results, 2020 Technology Spending Intentions Survey, janvier 2020.

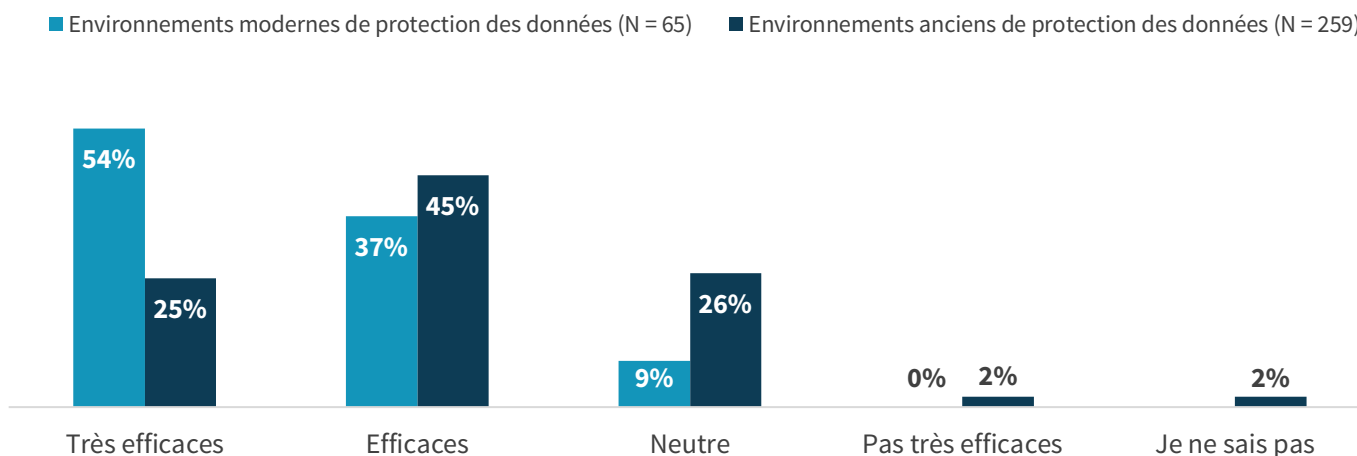
Figure 4. Efficacité des dépenses d'infrastructure sur site


Source : Enterprise Strategy Group

La protection des données « touche » tous les aspects de l'IT en raison de sa mission et de sa focalisation sur les données. Il semble logique que le fait d'avoir une solution de protection des données optimisée par défaut ou en tant qu'ajustement par rapport à une infrastructure en évolution contribue à l'efficacité opérationnelle au-delà de la simple protection des données. Comme le soulignent nos recherches, 91 % des départements IT dotés d'environnements de protection des données optimisés indiquent qu'ils sont efficaces pour générer de la valeur dans le cadre d'initiatives de Cloud hybride (voir Figure 5). Lorsque les besoins en matière de protection des données sont satisfaits et complètement intégrés de manière transparente dans tous les environnements, l'IT devient non seulement salvateur, mais il libère également un temps essentiel pouvant être affecté à d'autres fins, comme le fonctionnement de l'entreprise et le lancement de nouvelles initiatives.

Figure 5. Initiatives de Cloud hybride et stockage moderne : une combinaison plus efficace

En règle générale, comment évalueriez-vous l'efficacité des initiatives de Cloud hybride de votre entreprise pour générer de la valeur pour l'organisation ? (Part de répondants, par environnement de protection des données sur site)

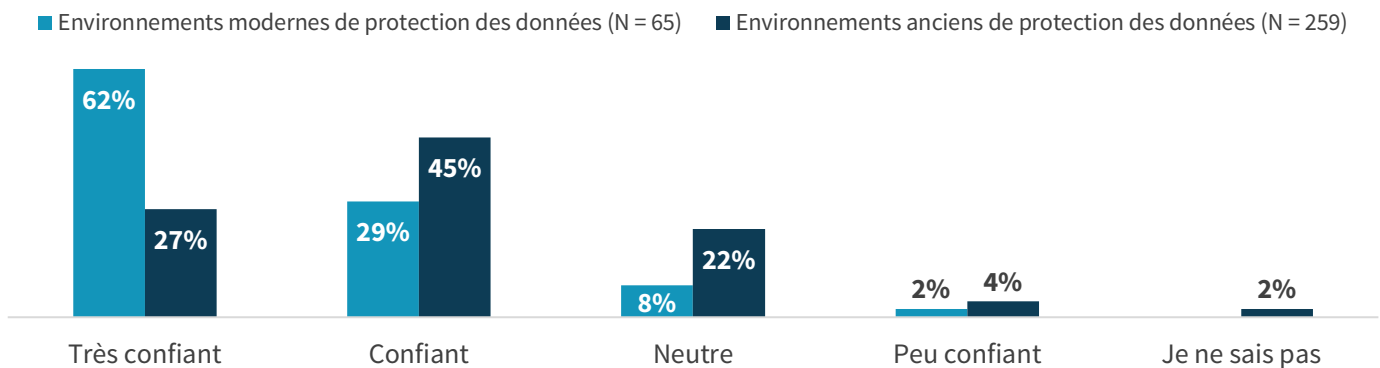


Source : Enterprise Strategy Group

En outre, les succès obtenus par le passé dans la réalisation des objectifs en matière de Cloud hybride grâce à une protection des données optimisée se traduisent par un niveau de confiance globalement plus élevé dans la capacité d'une entreprise à réaliser ses objectifs de Cloud hybride à l'avenir (voir Figure 6). Trois cinquièmes (62 %) des entreprises dotées d'environnements de protection des données optimisés sont très confiantes dans leur capacité à réaliser leurs objectifs de Cloud hybride au cours des 3 prochaines années, soit une fréquence 2,3 fois supérieure à celle des anciennes installations de protection des données (voir Figure 7). En outre, les départements IT d'installations modernes de protection des données sont 48 % plus susceptibles que leurs homologues dans des installations anciennes d'être considérés comme des facteurs de différenciation compétitifs par les dirigeants (40 % contre 27 %).

Figure 6. Contribution aux objectifs métiers du Cloud hybride : la confiance dans l'IT

Dans quelle mesure pensez-vous que votre département IT sera en mesure de contribuer aux objectifs de votre entreprise en matière de Cloud hybride au cours des 36 prochains mois ? (Part de répondants, par environnement de protection des données sur site)



Source : Enterprise Strategy Group

Ce qu'il faut retenir

Les infrastructures optimisées de protection des données constituent un facteur de réussite vis-à-vis des environnements de Cloud hybride et influencent le succès commercial, financier et technique au-delà de la simple protection des données. Pour une entreprise, l'amélioration et l'optimisation des technologies de protection des données sont une étape clé contribuant au succès de ses initiatives de Cloud hybride.

La protection des données est un excellent moyen d'apprentissage de l'IT, car elle englobe une multitude de disciplines et doit être mise en œuvre par rapport à des RPO et des RTO pouvant être rigoureux afin de soutenir l'entreprise et les nombreuses applications sur lesquelles elle s'appuie. Les meilleures pratiques et les compétences issues de cet effort peuvent être appliquées à de nombreux autres projets.

Cela se traduit par une amélioration des capacités à réussir dans les environnements de Cloud hybride, tout en augmentant la confiance au niveau des dirigeants. Ce « cercle vertueux » peut également être présent dans d'autres domaines. Il est intéressant de noter qu'en comparaison avec les entreprises disposant d'une infrastructure de protection des données ancienne, celles qui bénéficient d'une infrastructure de protection des données optimisée indiquent également des résultats positifs sur les projets Cloud en général, et leurs initiatives de Cloud hybride ont une valeur supérieure.

L'avenir de l'IT réside dans les topologies de Cloud hybride, et c'est dans ce domaine que des innovations continues sont attendues dans le cadre de la protection des données.

Comment Dell Technologies peut vous aider

Ce rapport Research Insights d'ESG a été commandé par les sociétés Dell Technologies, VMware et Intel Corporation, lesquelles concentrent leurs efforts pour aider les organisations à atteindre leurs objectifs en matière de Cloud.

Ensemble, Dell Technologies, VMware et Intel Corporation favorisent l'innovation et les fonctionnalités de nouvelle génération avec une gamme exceptionnelle de solutions de confiance en matière d'infrastructure, de Cloud et de protection des données. Cette gamme complète de matériel, de logiciels et de services permet aux entreprises d'adopter facilement des technologies de transformation afin d'optimiser leurs performances, de rivaliser et de prospérer dans la nouvelle économie numérique.

Les solutions de protection des données Dell EMC pour le Cloud, le multi-Cloud et le Cloud hybride aident les clients à transformer leurs datacenters afin d'améliorer l'efficacité opérationnelle, la résilience et l'évolutivité sur l'ensemble de leur infrastructure de type Cloud. En outre, Dell Technologies On Demand propose la gamme de solutions de bout en bout basées sur la consommation et as-a-service la plus étendue du secteur, parfaitement adaptée aux modes de consommation des services et de l'infrastructure sur site dans l'économie à la demande moderne.

Pour en savoir plus sur les solutions de protection des données Dell EMC pour le Cloud, cliquez [ici](#).

Annexe : méthodologie de recherche et caractéristiques démographiques des personnes interrogées

Pour collecter les données de ce rapport, ESG a mené une enquête en ligne complète auprès de décideurs IT au sein d'organisations des secteurs privé et public dans 11 pays : Allemagne (7 %), Australie (5 %), Brésil (8 %), Canada (4 %), États-Unis (33 %), France (9 %), Hong Kong (3 %), Inde (4 %), Mexique (8 %), Royaume-Uni (13 %) et Singapour (5 %). L'enquête a été réalisée entre le 17 septembre 2019 et le 12 octobre 2019. Pour être admissibles à cette enquête, les personnes interrogées devaient avoir un pouvoir décisionnaire sur les investissements dans le Cloud (public ou privé) au sein d'entreprises utilisant une infrastructure de type Cloud public et exploitant des environnements de datacenter modernisés sur site.

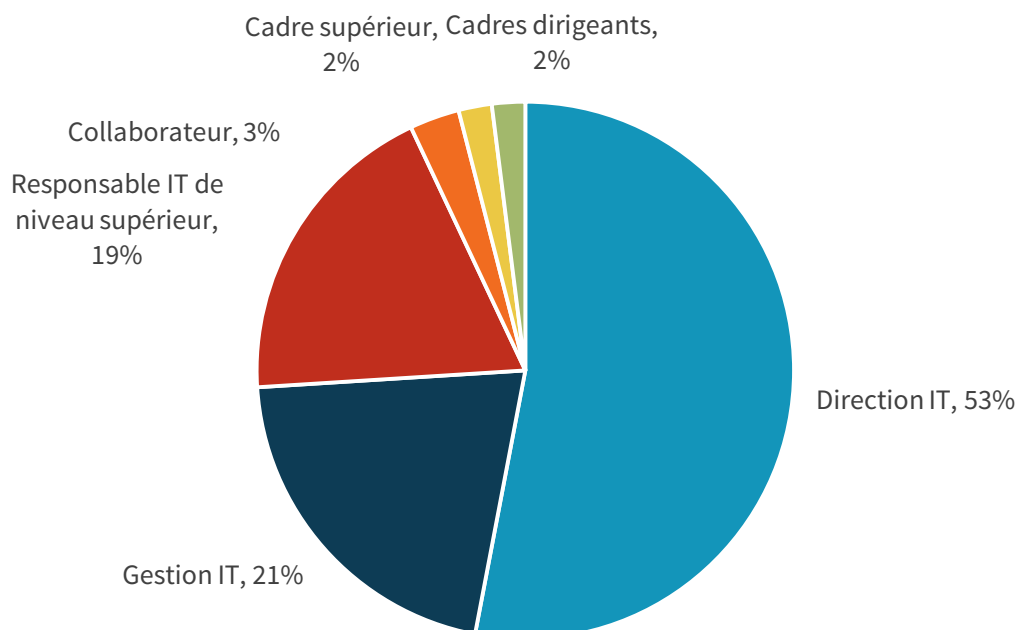
Après avoir éliminé les participants non éligibles, supprimé les doublons et analysé les réponses complètes restantes (sur la base de plusieurs critères) en vue d'assurer l'intégrité des données, il est resté un échantillon final de 1 257 participants.

Toutes les personnes interrogées ont reçu un incentive pour répondre à l'enquête, sous la forme d'une récompense et/ou somme en espèces. Remarque : Il est possible que le résultat de l'addition des totaux des figures et des tableaux de ce rapport ne soit pas égal à 100 %, en raison de l'arrondi.

Les figures ci-dessous décrivent en détail les données démographiques de la base de personnes interrogées : responsabilités actuelles de chaque personne interrogée, nombre total de collaborateurs, principal secteur d'activité des entreprises des personnes interrogées.

Figure 7. Participants à l'enquête, par intitulé/niveau de poste

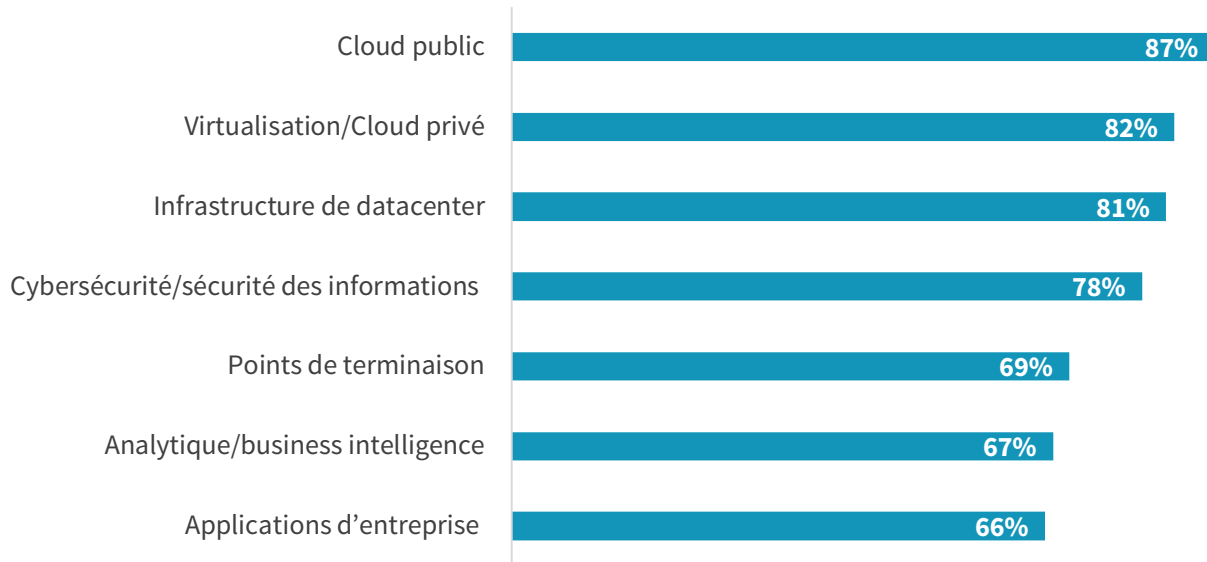
Laquelle de ces propositions décrit le mieux l'intitulé/le niveau actuel de votre poste ? (Part de répondants, N = 1 257)



Source : Enterprise Strategy Group

Figure 8. Personnes interrogées pendant l'enquête, par domaine de responsabilité informatique

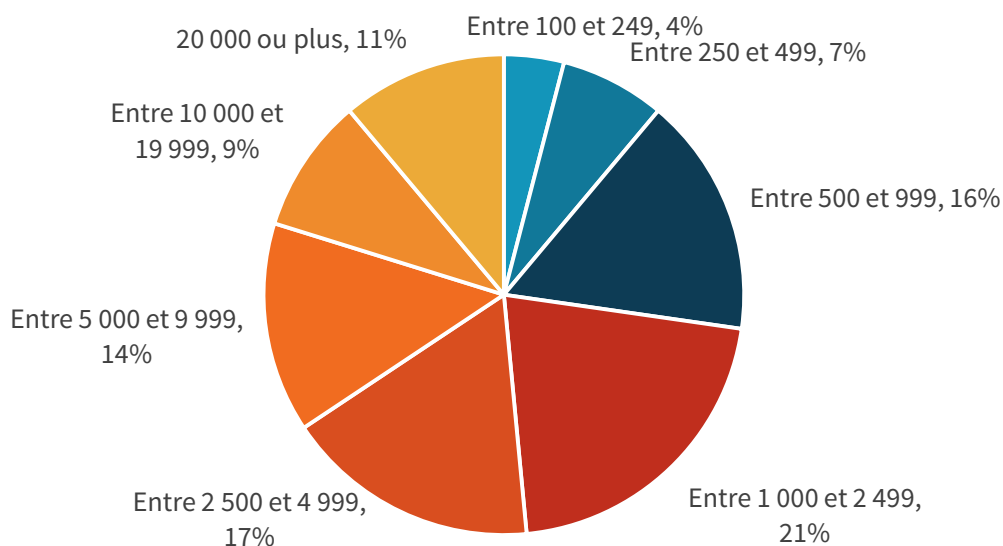
Dans quels domaines de l'informatique êtes-vous impliqué de façon significative dans les processus d'achat de votre société ? (Part de répondants, N = 1 257, plusieurs réponses acceptées)



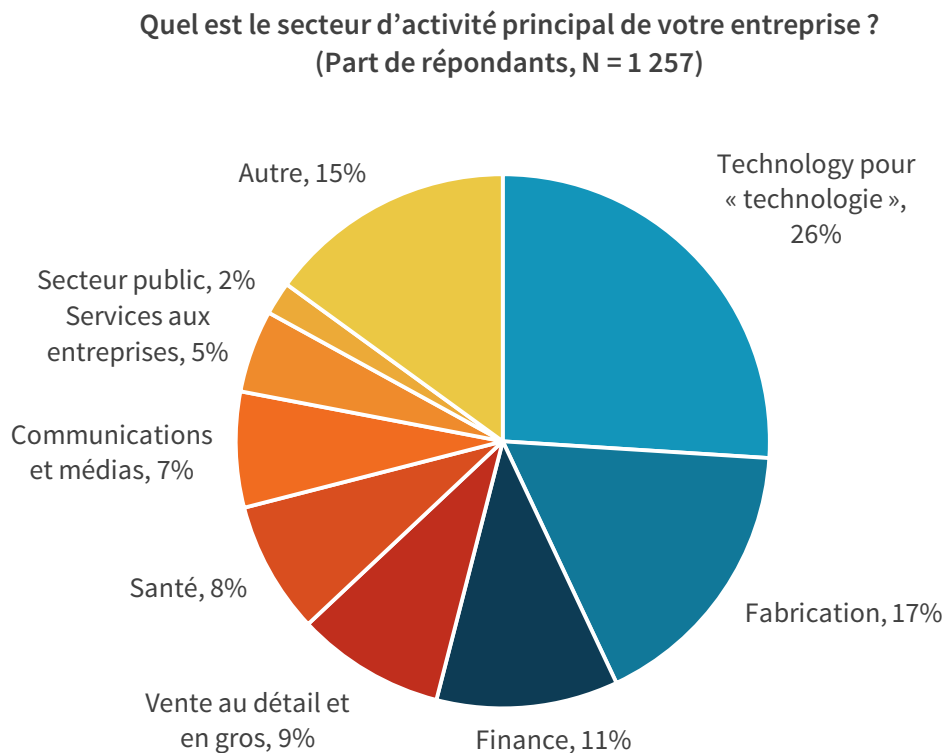
Source : Enterprise Strategy Group

Figure 9. Personnes interrogées pendant l'enquête, par taille de société (nombre de collaborateurs)

Quel est le nombre total de collaborateurs dans votre entreprise à travers le monde ? (Part de répondants, N = 1 257)



Source : Enterprise Strategy Group

Figure 10. Personnes interrogées pendant l'enquête, par secteur

Source : Enterprise Strategy Group

Toutes les marques sont la propriété de leurs sociétés respectives. The Enterprise Strategy Group (ESG) considère que les informations contenues dans cette publication proviennent de sources connues comme fiables, mais ne garantit pas leur exactitude. Cette publication peut comporter des informations reflétant des opinions propres à ESG et qui sont susceptibles de changer. Enterprise Strategy Group, Inc. détient les droits de cette publication. Toute reproduction ou diffusion intégrale ou partielle au format papier, électronique ou autre, destinée à une personne non autorisée à la recevoir, sans accord exprès d'Enterprise Strategy Group, Inc., constitue une violation de la loi américaine sur le copyright, est passible de poursuites et peut entraîner des dommages-intérêts, ainsi qu'une condamnation pénale le cas échéant. Pour toute question, veuillez contacter le service client d'ESG au 508.482.0188.



Enterprise Strategy Group est une entreprise de recherche, de validation, de stratégie et d'analyse IT qui fournit des perspectives interactives et intelligentes à la grande communauté des technologies de l'information.