Global Data Protection Index - Édition spéciale 2024

Principales conclusions - Octobre 2023

VansonBourne

DELL Technologies

Portée des principales conclusions

1
L’environnement des risques en matière de protection des données

2
La menace croissante des cyberattaques

3
L’utilisation du multicloud

4
La sécurisation d’un environnement Cloud

Cinq points clés à retenir

Les cyberattaques continuent de proliférer

Les coûts liés aux cyberattaques augmentent

Les polices d’assurance ne couvrent pas l’intégralité des coûts liés aux attaques

L’utilisation accrue de l’IA générative peut renforcer la valeur des données

Cela intensifie les risques et les impacts financiers des cyberattaques

Qui avons-nous interrogé ?

1 500 décideurs informatiques et en sécurité informatique interrogés entre septembre et octobre 2023

Organisations provenant d'une vaste gamme de secteurs publics et privés

Organisations de plus de 250 collaborateurs

4 zones géographiques :

Amériques (300)
EMEA (675)
APJ (375)
Chine (150)

1. L’environnement des risques en matière de protection des données

Les préoccupations liées aux mesures de protection des données sont généralisées, et le moindre doute place les organisations dans une position vulnérable

60 %

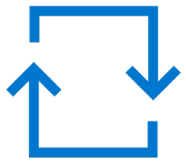
ne sont **pas vraiment convaincus** que leur organisation **atteint ses objectifs de niveau de service en matière de sauvegarde et de restauration**

79 %

craignent qu'un **événement d'interruption se produise** dans les douze prochains mois

75 %

craignent que les mesures de protection des données de leur organisation **ne soient pas suffisantes pour faire face aux menaces des logiciels malveillants et des ransomwares**

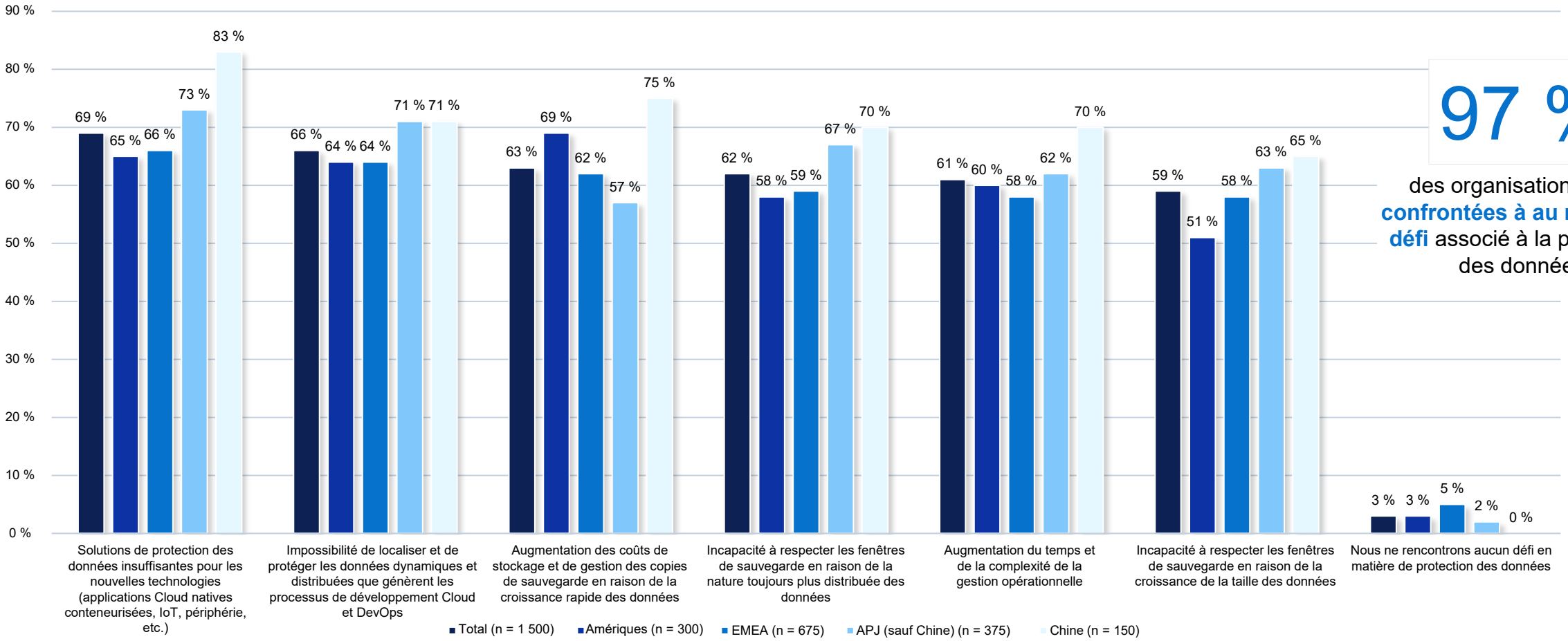


65 %

ne sont **pas vraiment sûrs** que leur organisation soit capable de **restaurer entièrement les systèmes/données de toutes leurs plateformes** en cas de perte de données

Outre ces préoccupations liées à la protection des données, de nombreuses organisations sont confrontées à plusieurs défis

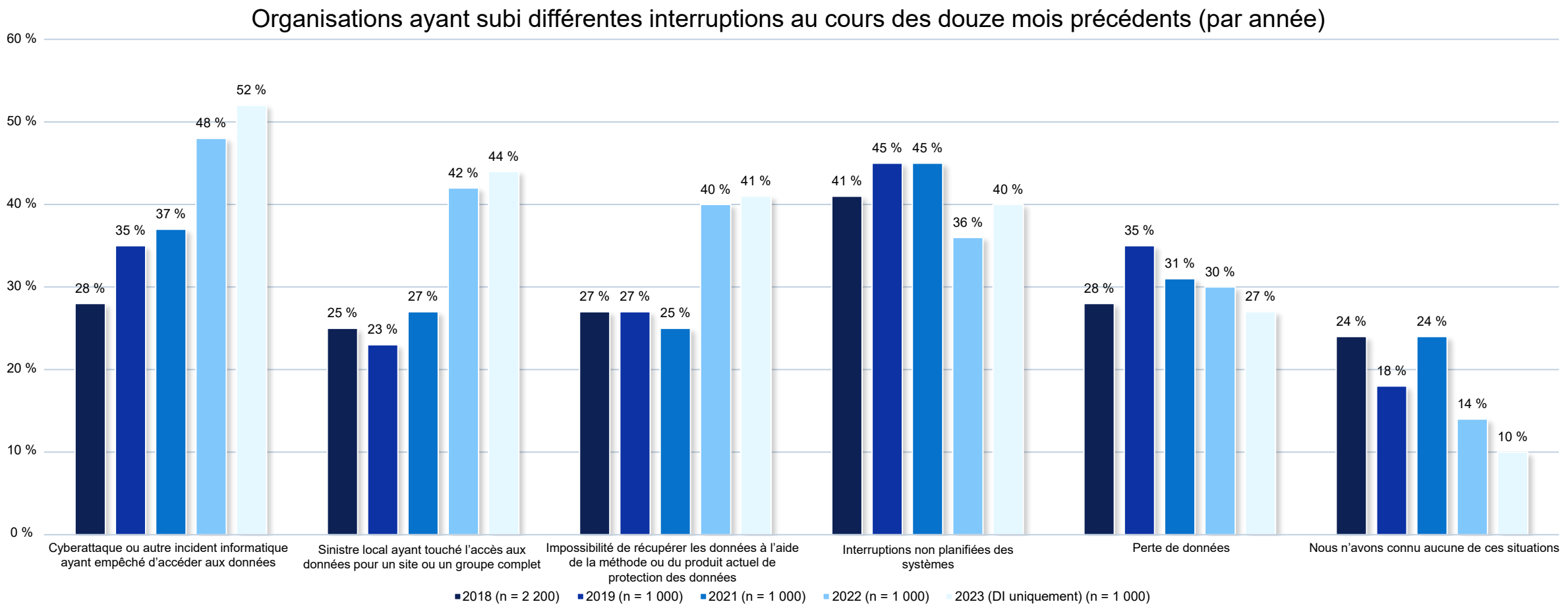
Les 5 principaux défis liés à la protection des données (par zone géographique)



97 %

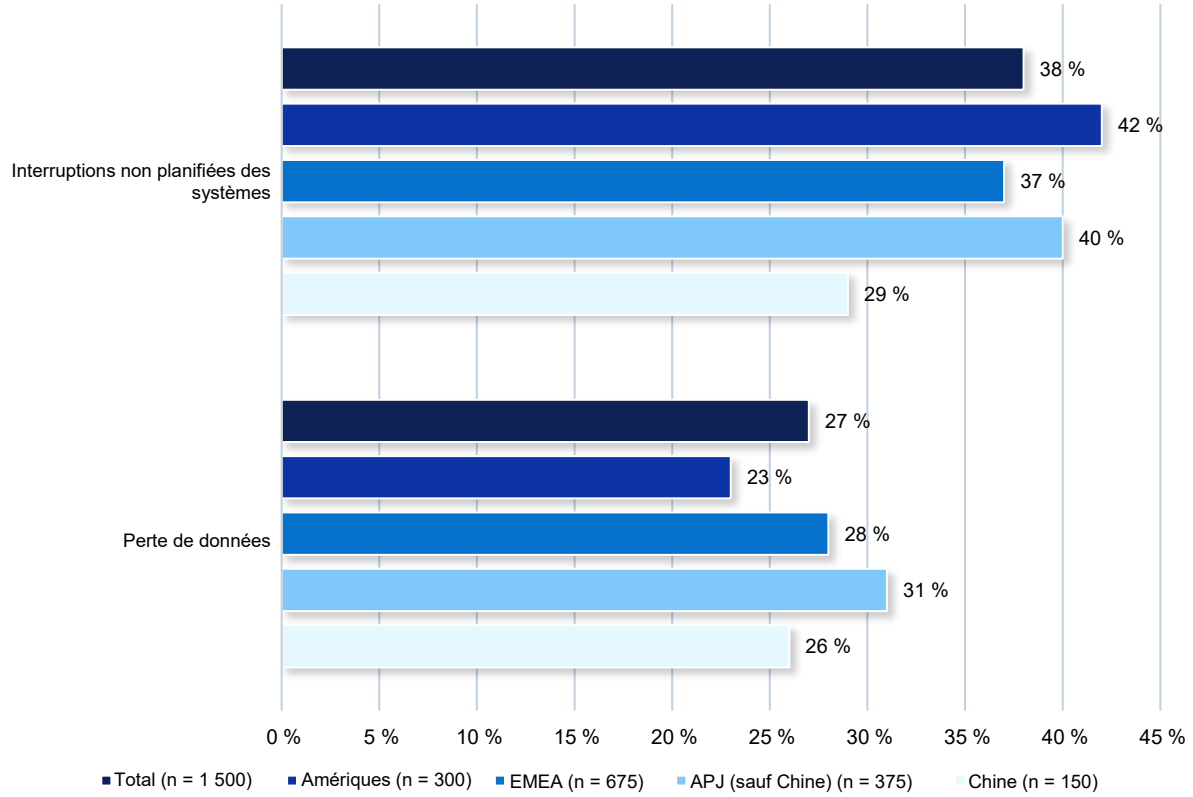
des organisations **sont confrontées à au moins un défi** associé à la protection des données

Ces douze derniers mois, les organisations ont subi d'importantes interruptions, les cyberattaques constituant une menace grandissante toujours plus présente



Les pertes de données ont non seulement provoqué une interruption, mais elles ont également affecté les résultats

Organisations ayant subi des pertes de données ou des interruptions de service des systèmes non planifiées au cours des douze mois précédents (pourcentage par zone géographique)



Au cours des 12 derniers mois :

26 heures

d'interruption de service des systèmes non planifiée enregistrées en moyenne

2,45 To

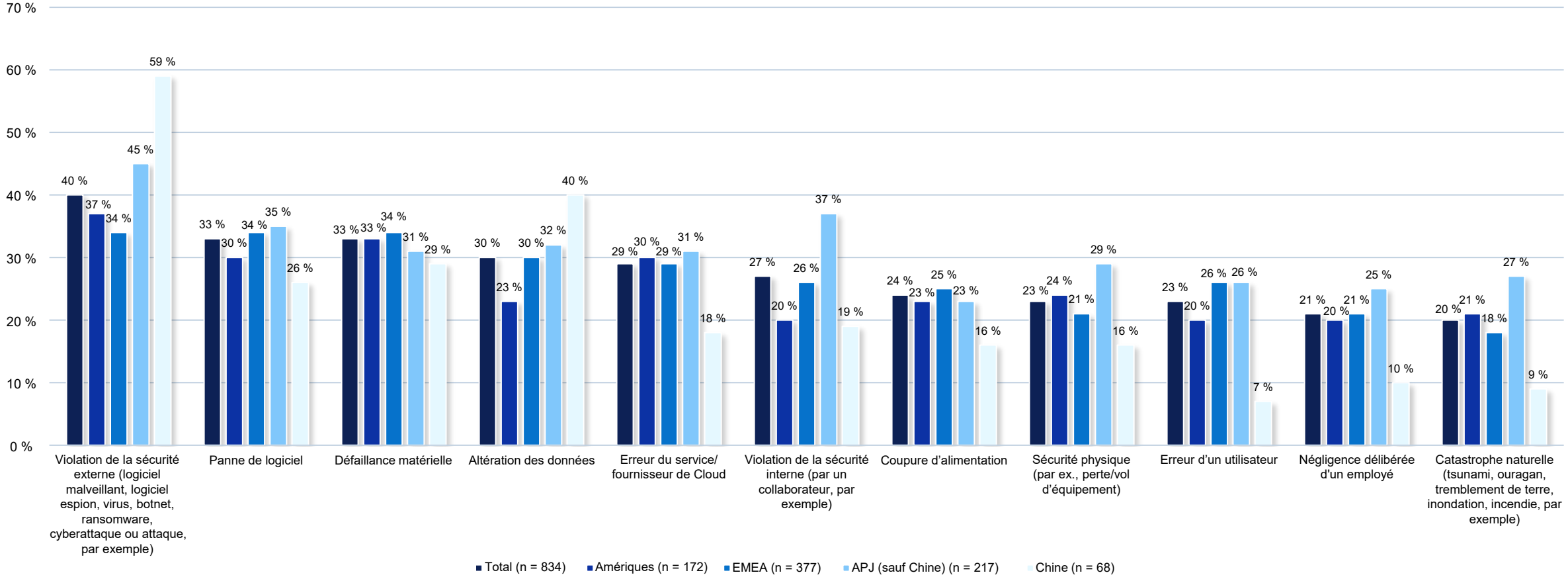
de données perdues en moyenne

2,61 millions de $

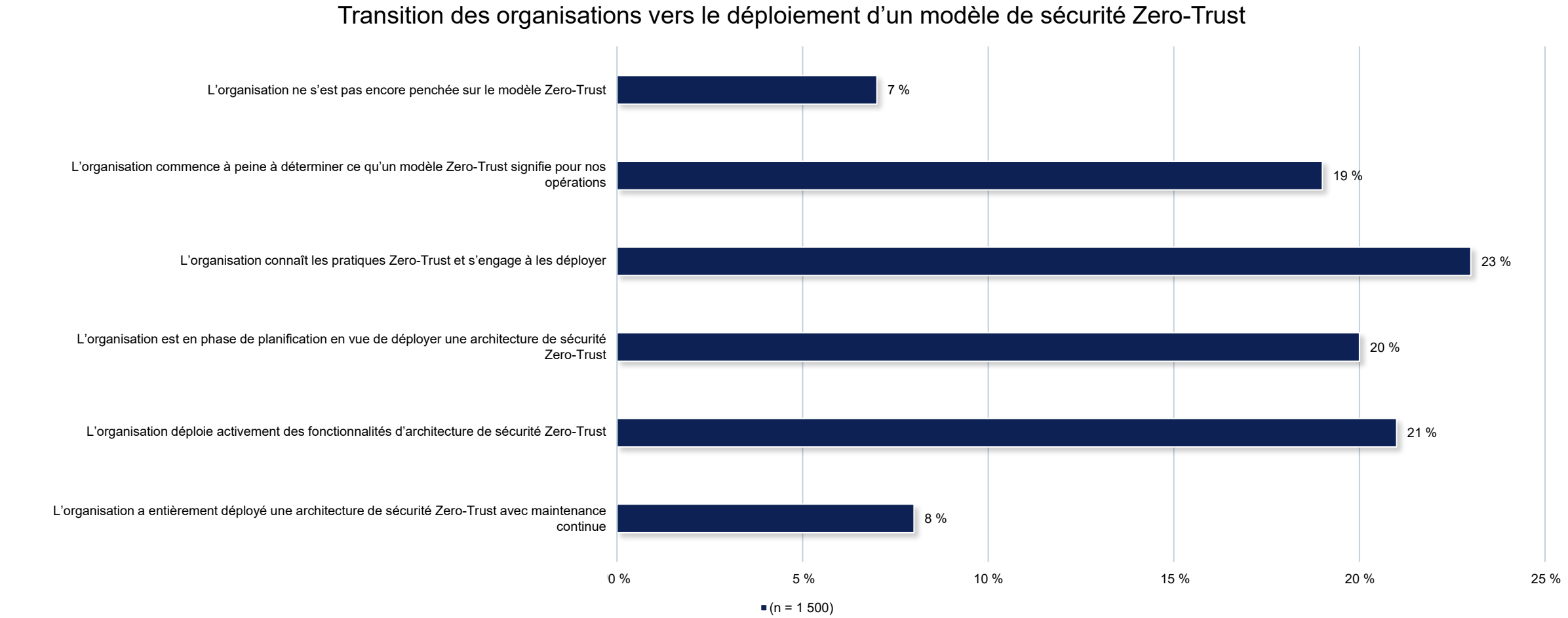
de coût relevé en moyenne **pour une perte de données**

Les menaces de sécurité externes constituent les causes les plus fréquentes à l'origine des pertes de données et/ou des interruptions de service non planifiées au cours des douze derniers mois

Causes à l'origine des pertes de données et/ou des interruptions de service au cours des douze derniers mois



Malgré les défis et les préoccupations liés à la protection des données, peu d'entre elles ont entièrement déployé un modèle de sécurité Zero-Trust

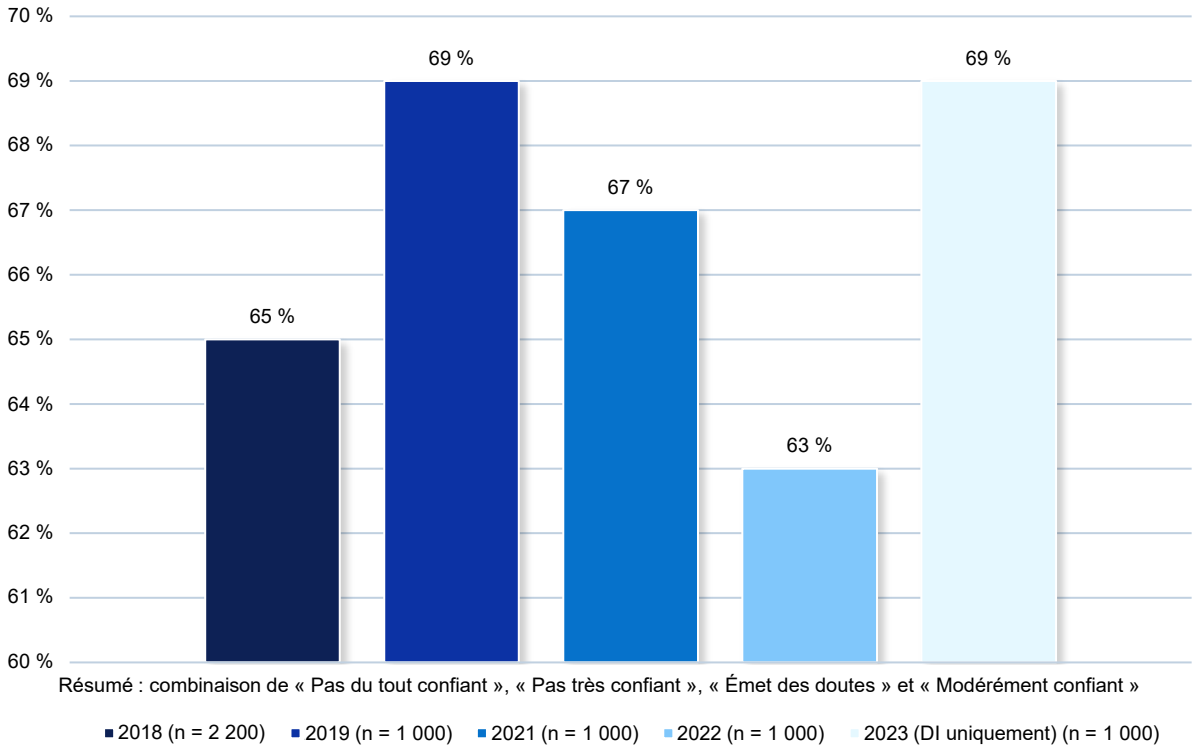


Filtre : répartition des données par zone géographique (total)

2. La menace croissante des cyberattaques

Les préoccupations liées aux mesures de protection des données sont généralisées, et le moindre doute place les organisations dans une position vulnérable

Organisations pas vraiment sûres de pouvoir récupérer toutes les données stratégiques de l'entreprise en cas de cyberattaque destructrice (par année)



81 %

considèrent que leur organisation est **plus exposée aux pertes de données dues aux cybermenaces** à cause du nombre croissant de télétravailleurs

74 %

craignent que leurs données de sauvegarde soient **infectées ou corrompues suite à une attaque par ransomware**

À ce risque vient s'ajouter un excès de confiance autour des conséquences d'une attaque par ransomware

72 %

considèrent que le travail et les collaborateurs de l'organisation **ne seront pas affectés par une attaque par ransomware**

74 %

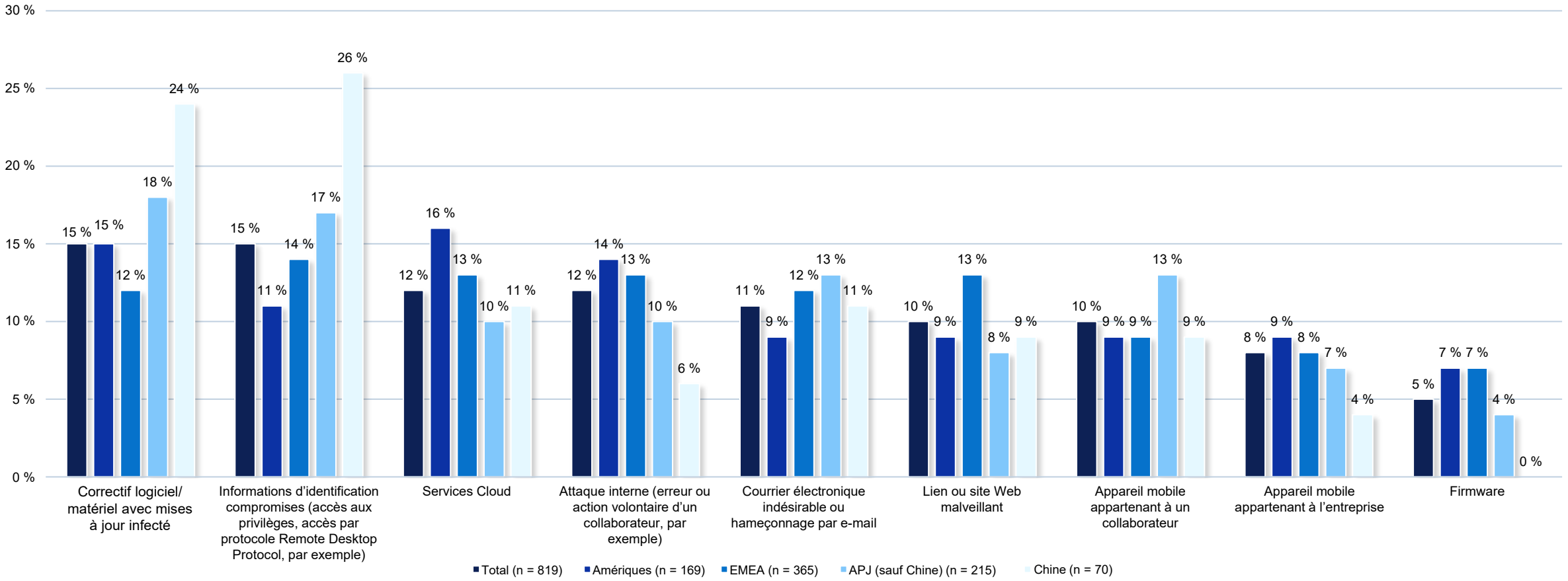
considèrent qu'en cas d'attaque par ransomware, leur organisation récupérera **toutes les données** et reprendra ses activités **si elle paie la rançon**

66 %

considèrent qu'en cas d'attaque par ransomware, leur organisation **ne sera plus attaquée** une fois qu'elle aura payé la rançon

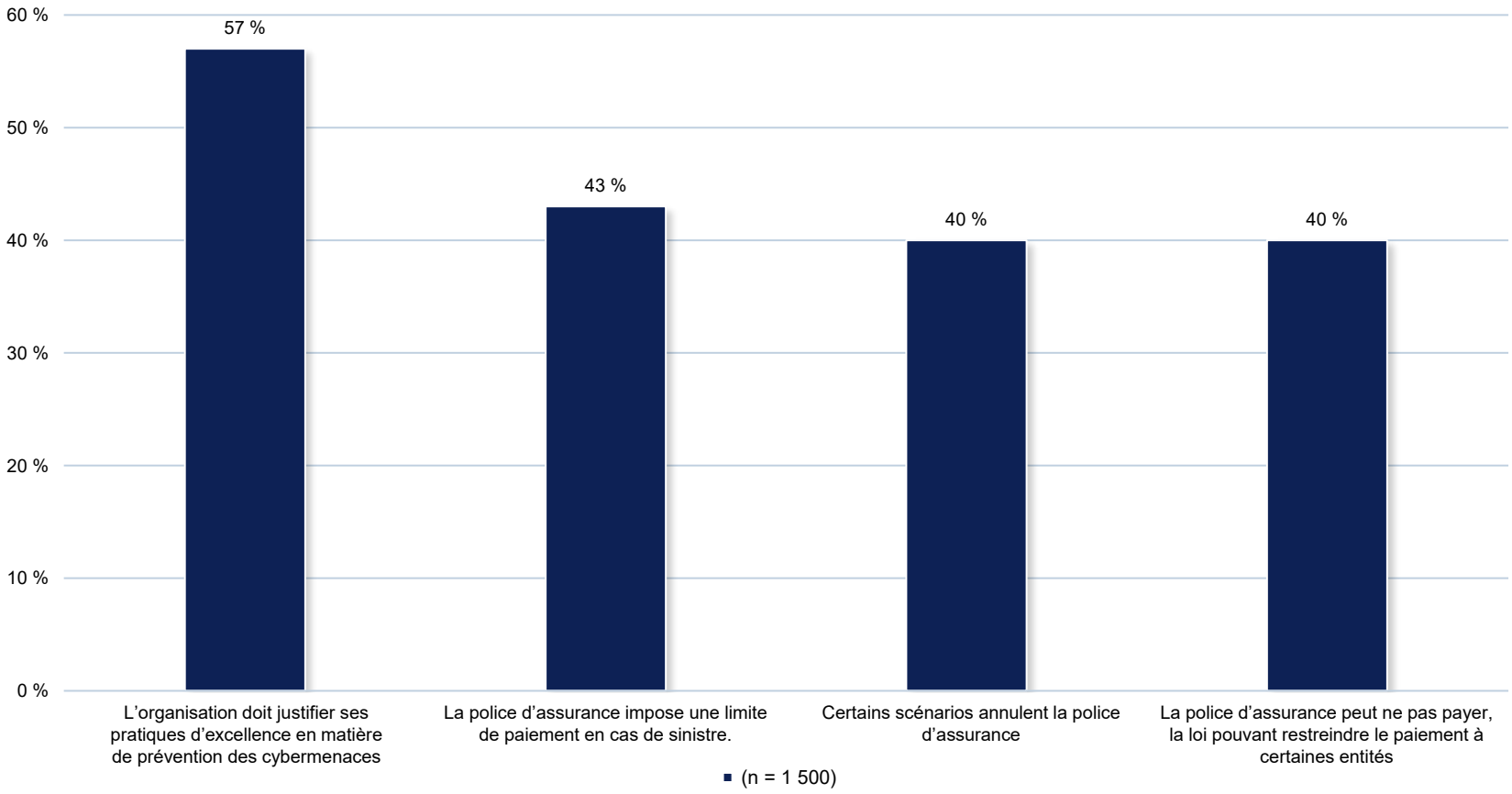
Les cybercriminels ciblent plusieurs points d'entrée, avec des attaques plus susceptibles de provenir de sources externes

Point d'entrée de la dernière cyberattaque des organisations (par zone géographique)



Même si les polices d'assurance contre les ransomwares sont monnaie courante, elles font l'objet de nombreuses réserves

Conditions des polices d'assurance contre les ransomwares des organisations

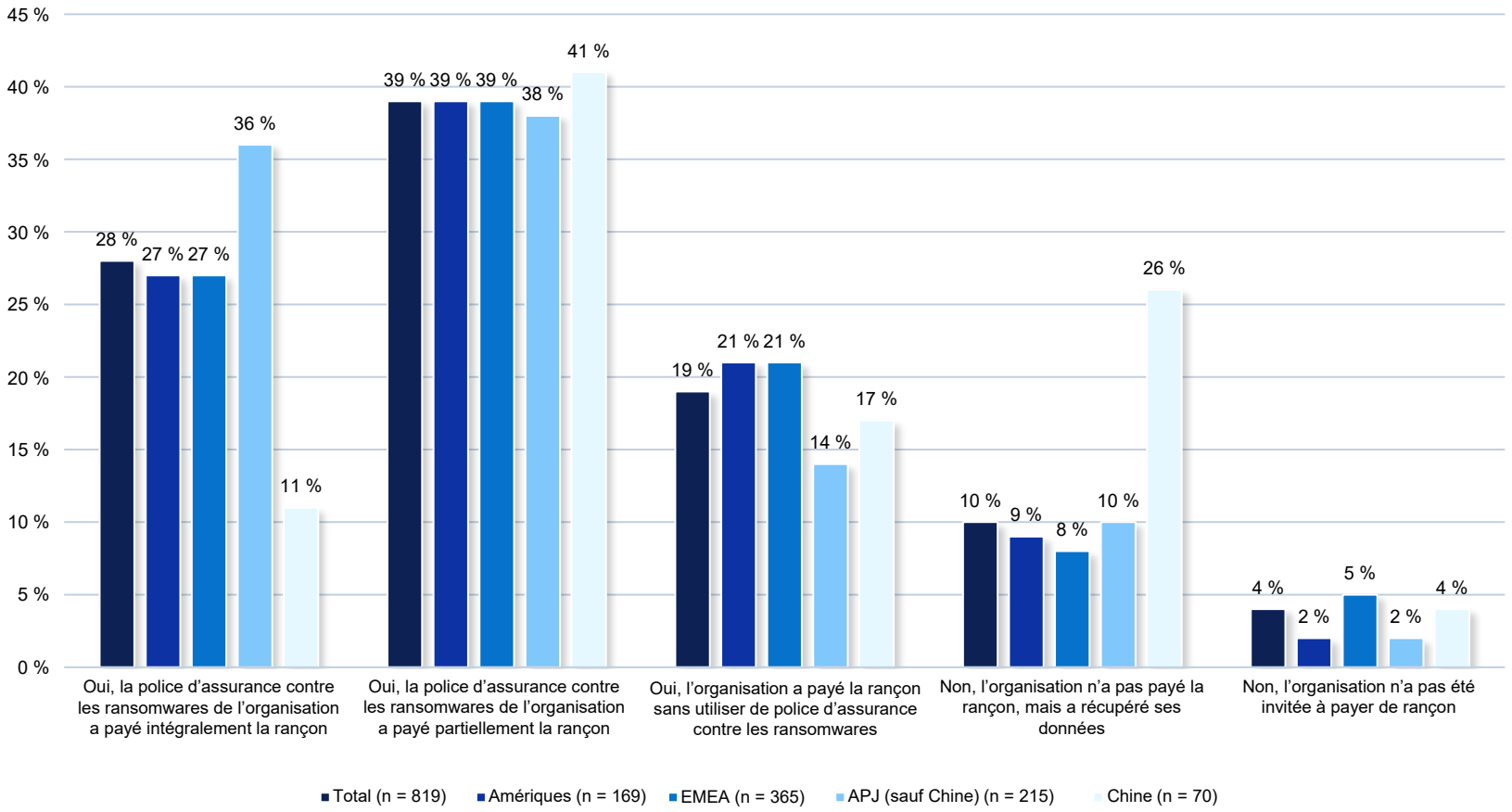


93 %

des organisations **ont une police d'assurance contre les ransomwares**

Même si bon nombre d'entre elles ont souscrit une police d'assurance contre les ransomwares, les organisations demeurent vulnérables sur le plan financier

Rançon versée pour récupérer l'accès aux données de l'organisation (par zone géographique)

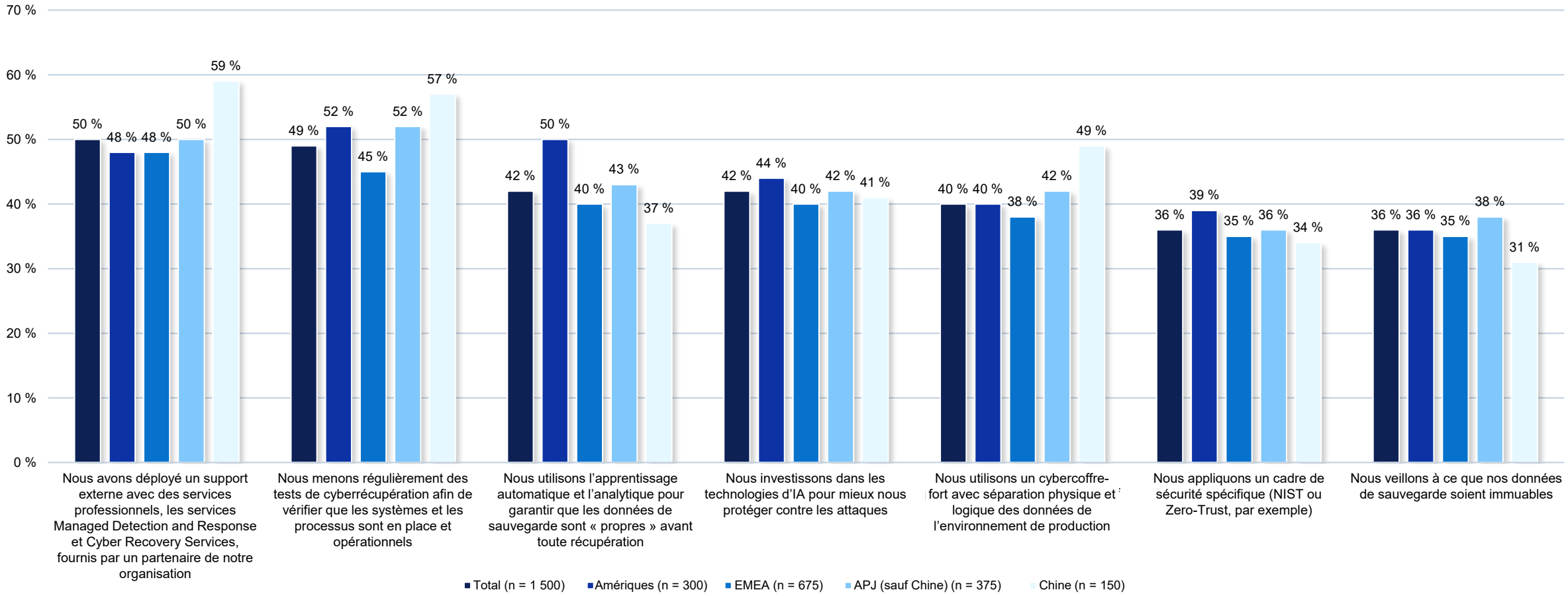


1,92 $

Mio de $: coût moyen engendré par les **cyberattaques et les incidents informatiques** pour les organisations au cours des douze derniers mois

De manière encourageante, les organisations prennent des mesures pour asseoir leur cyberrésilience

Mesures adoptées par les organisations pour renforcer leur cyberrésilience (par zone géographique)

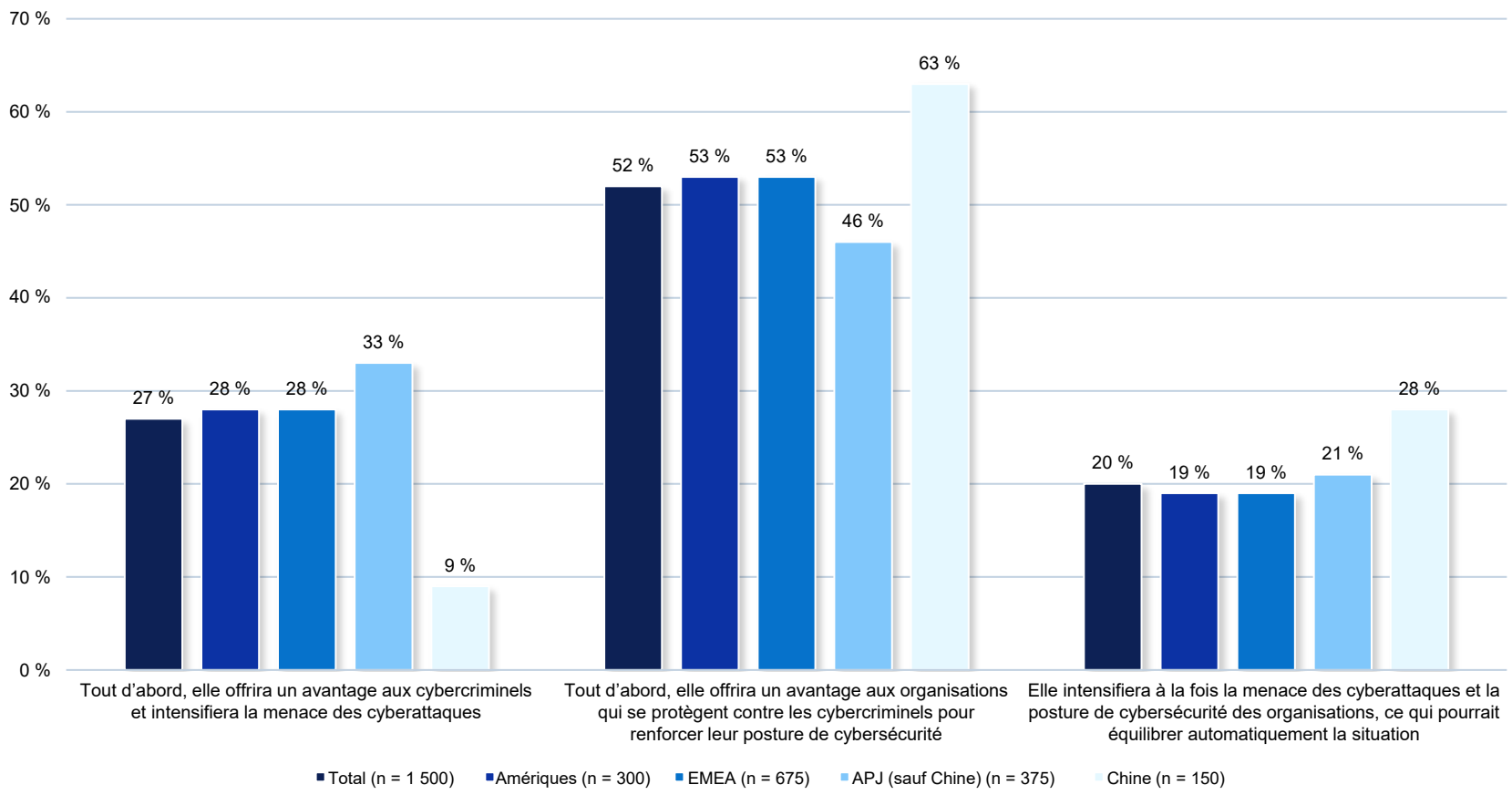


Toutefois, toutes ne croient pas que l'IA générative servira leur cyberrésilience

81 %

considèrent que les technologies émergentes (comme l'IA, l'IoT, la périphérie) **présentent un risque pour la protection des données**

Impact de l'IA générative sur les cybermenaces et la sécurité des données (par zone géographique)



Parmi les organisations ayant déjà beaucoup à faire avec la protection des données, bon nombre d'entre elles croient que l'IA générative va créer de nouveaux défis

88 %

considèrent que l'IA générative va créer d'importants volumes de données nouvelles qu'il faudra **protéger et sécuriser**

88 %

considèrent que l'IA générative va augmenter la valeur de certains types de données, ce qui peut **imposer des niveaux de service de protection des données plus élevés**

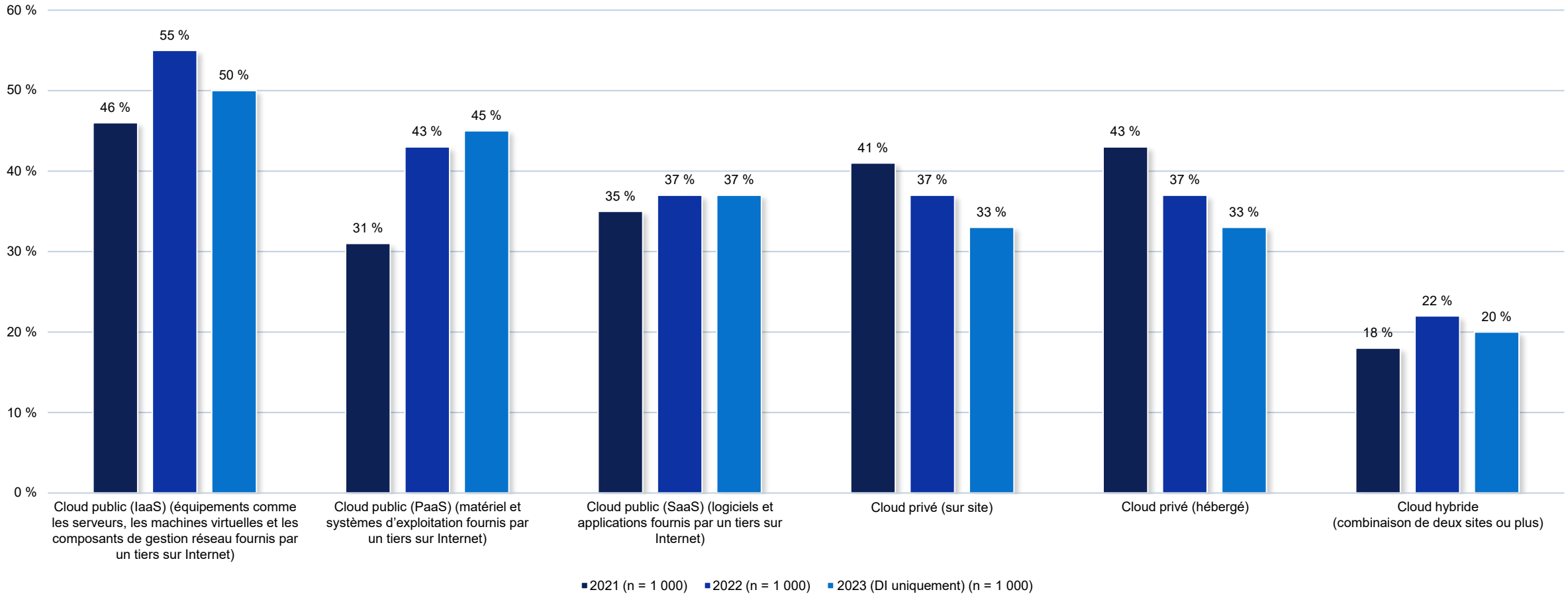
85 %

considèrent que la **corruption** des jeux de données utilisés pour l'IA générative **affectera les résultats de l'IA générative**

3. L’utilisation du multicloud

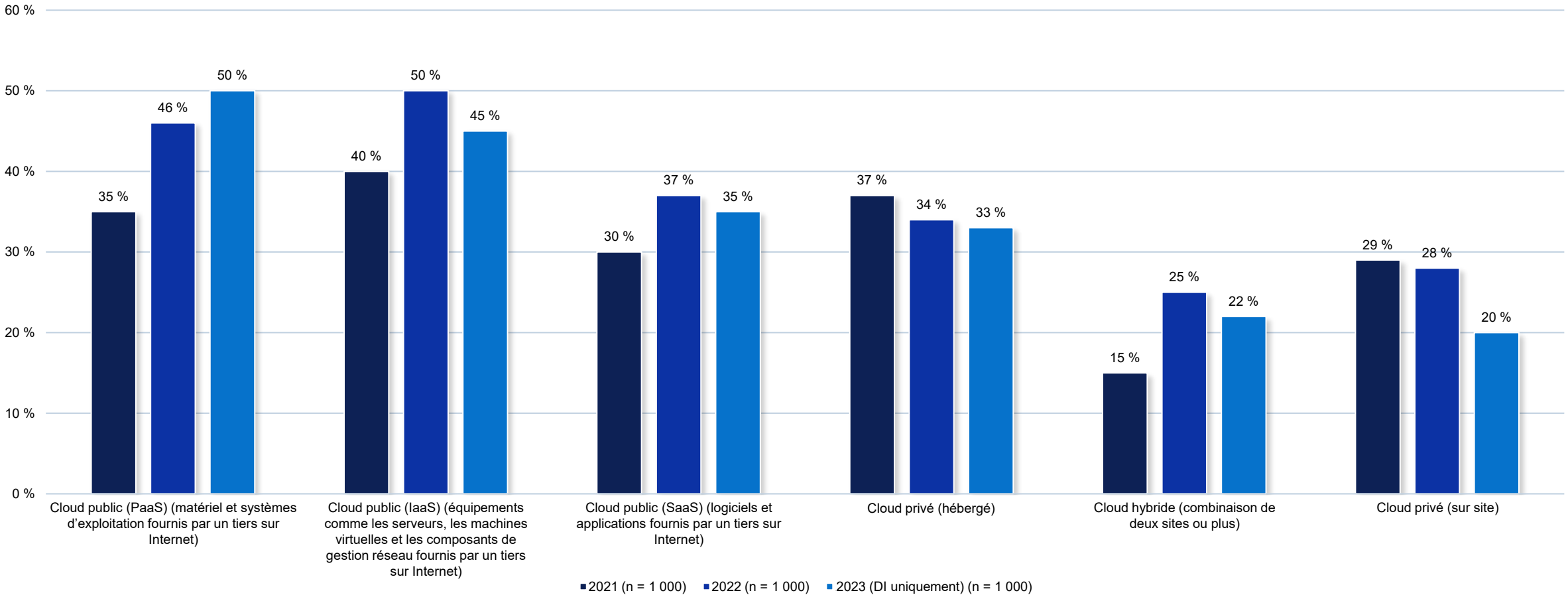
Alors que la préférence pour le Cloud privé diminue, le Cloud public reste un choix très prisé pour la mise à jour des applications existantes

Orientation choisie pour la mise à jour d'applications existantes (par année)

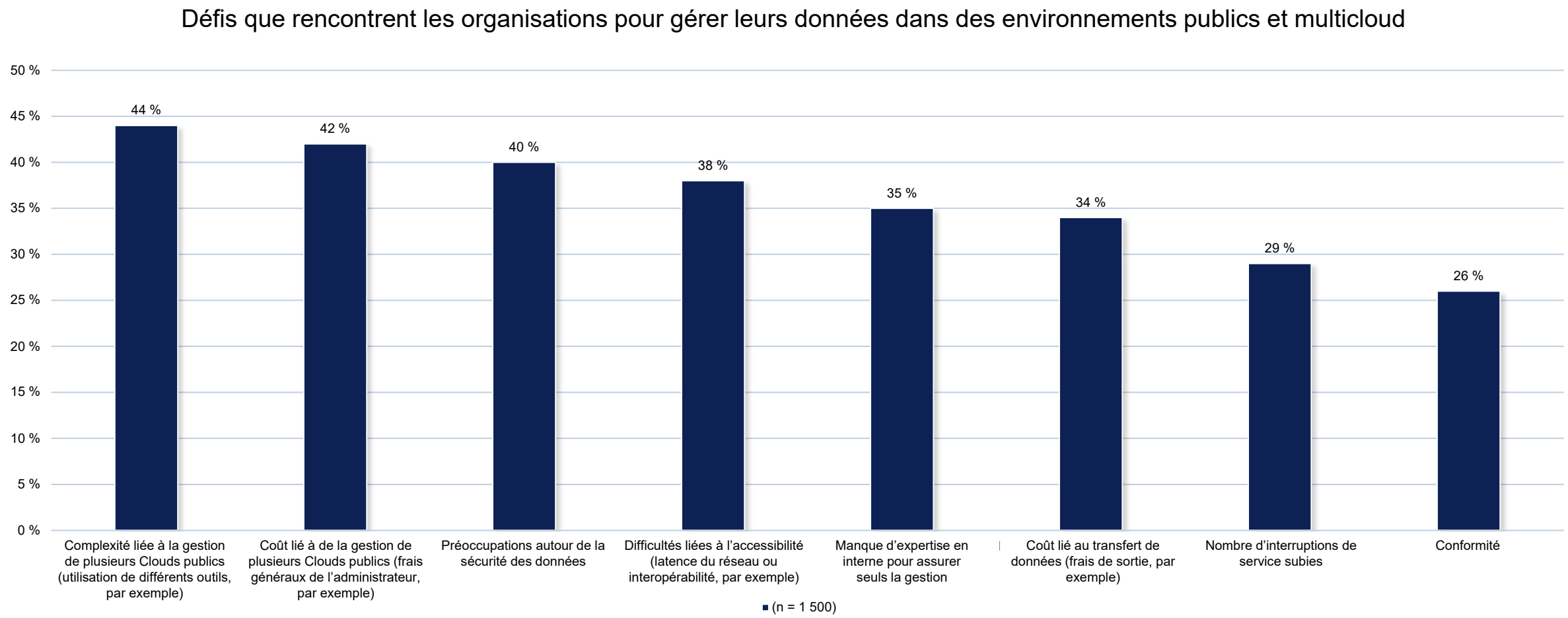


Le Cloud public reste également un choix très prisé pour le déploiement de nouvelles applications, même si le support diminue

Orientation choisie pour le déploiement de nouvelles applications (par année)



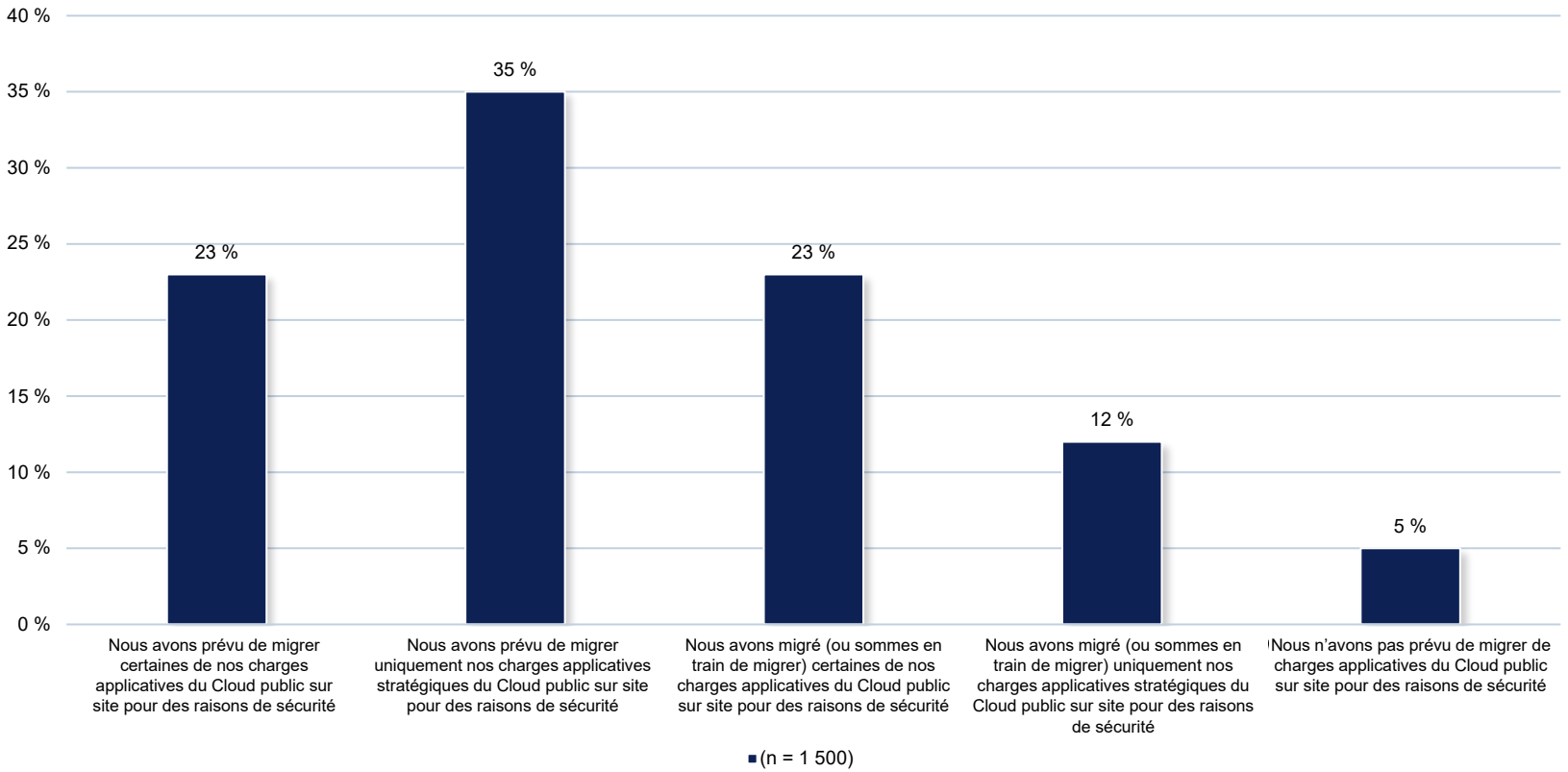
Malgré la popularité du Cloud public, de nombreuses organisations rencontrent des défis pour gérer leurs données



Filtre : répartition des données par zone géographique (total)

Face aux préoccupations en matière de sécurité, de nombreuses organisations migrent (ou ont prévu de migrer) une partie de leurs charges applicatives du Cloud public sur site

Part de la migration des charges applicatives du Cloud public sur site par les organisations



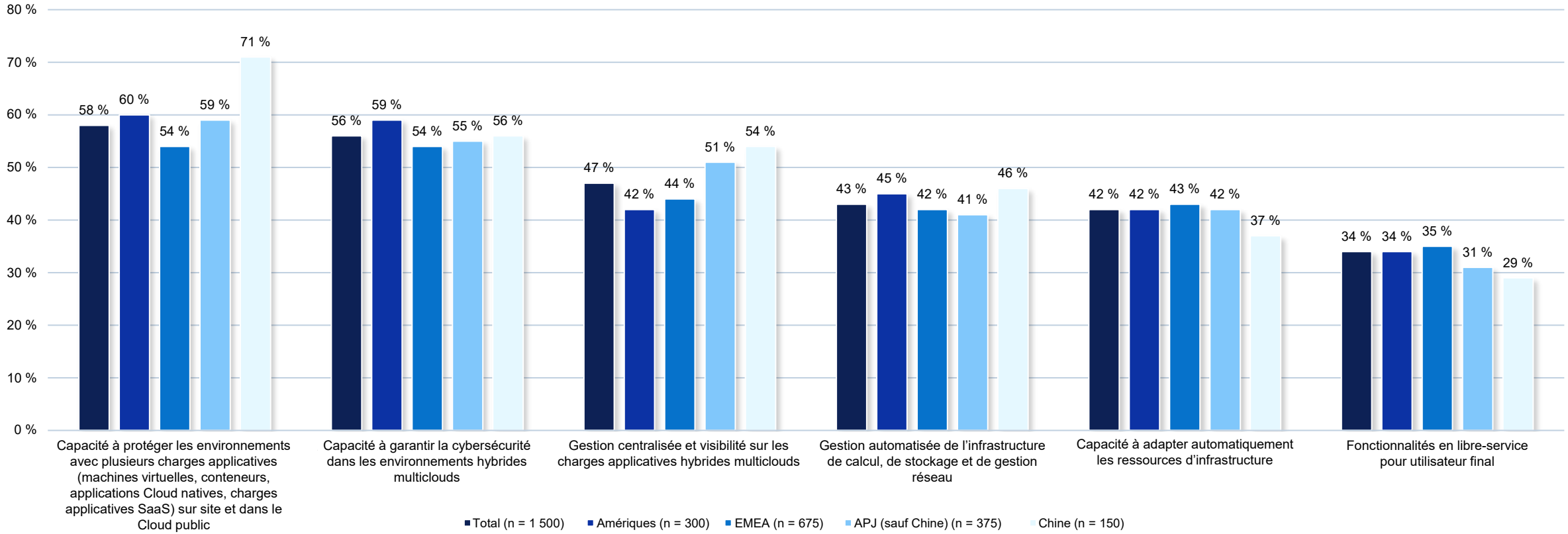
79 %

ne sont **pas vraiment sûrs** que leur organisation peut **protéger toutes ses données** dans les environnements de Cloud public

Filtre : répartition des données par zone géographique (total)

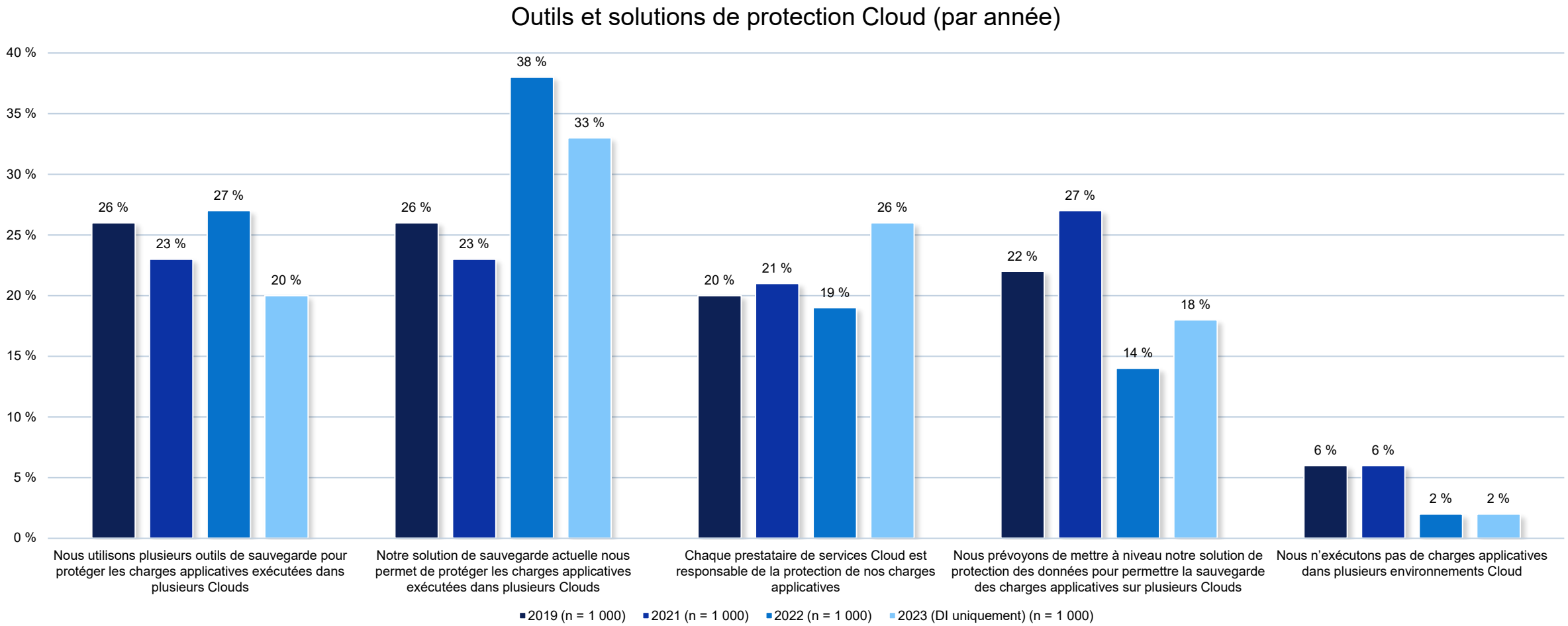
Face à l'intensification des cyberincidents et à la confiance érodée dans les stratégies de protection des données, bon nombre d'entre elles considèrent la sécurité comme une composante essentielle des opérations hybrides multiclouds

Fonctionnalités essentielles des opérations hybrides multiclouds (par zone géographique)



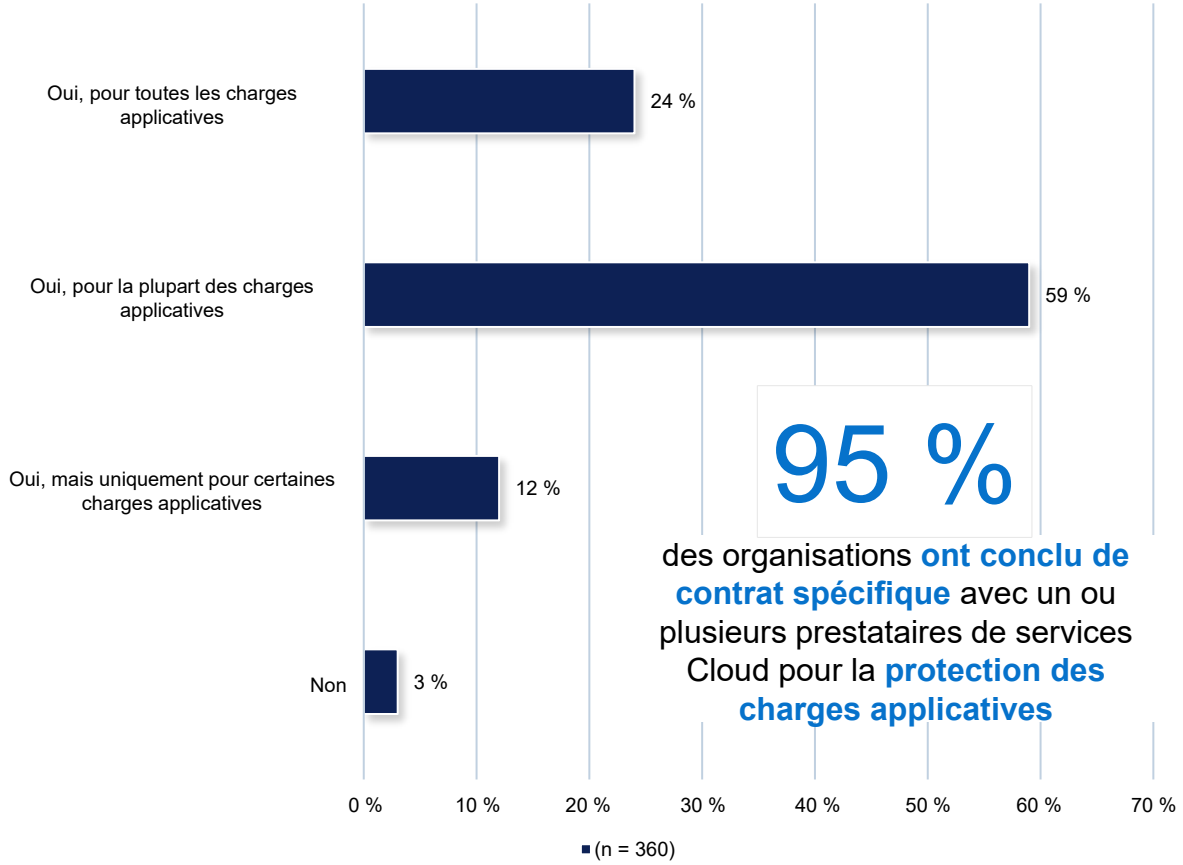
4. La sécurisation d’un environnement Cloud

À l'heure actuelle, les organisations utilisent plusieurs outils et solutions de sauvegarde pour protéger leurs charges applicatives, même si des mises à niveau sont nécessaires



Les organisations dépendent de plus en plus des prestataires de services Cloud pour protéger leurs charges applicatives dans les environnements Cloud

Contrat indépendant avec le CSP pour la protection des charges applicatives

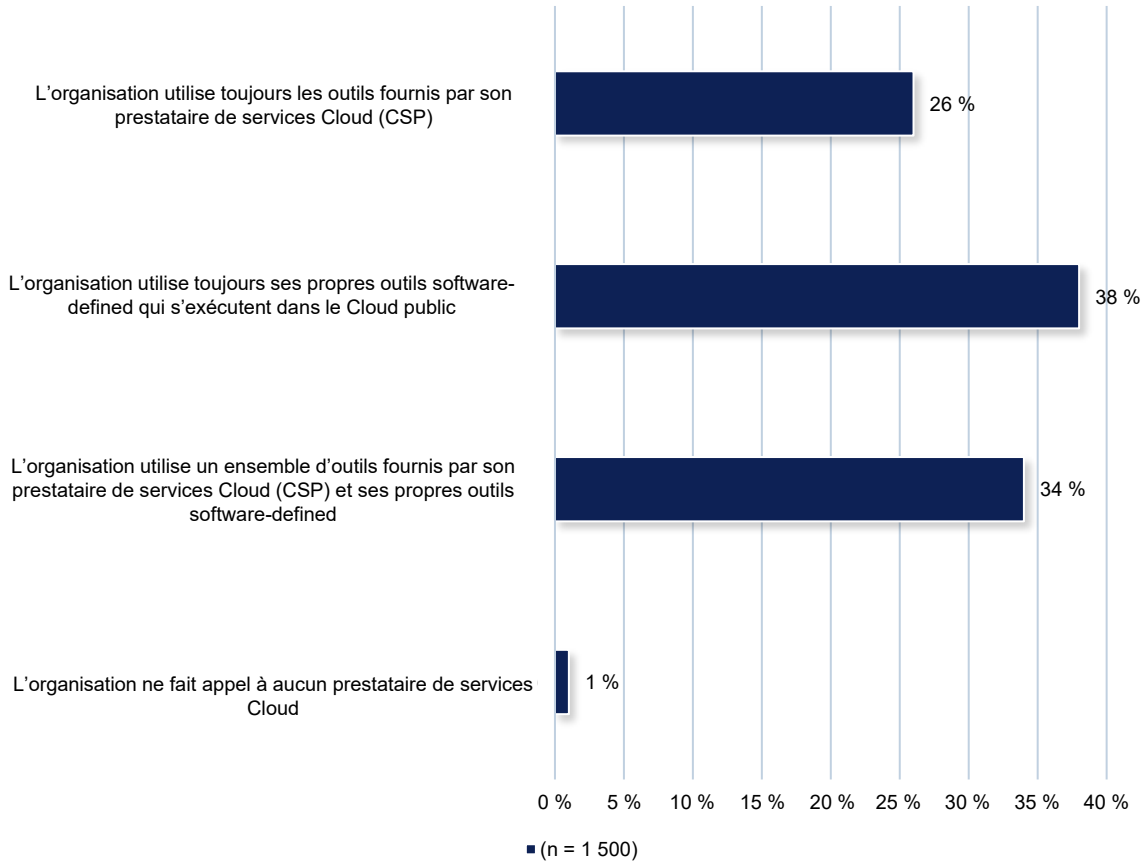


95 %

des organisations **ont conclu de contrat spécifique** avec un ou plusieurs prestataires de services Cloud pour la **protection des charges applicatives**

Filtre : répartition des données par zone géographique (total)

Outils de sauvegarde et de restauration fournis par le prestataire de services Cloud



Filtre : répartition des données par zone géographique (total)

Principales conclusions : en bref

L'environnement des risques en matière de protection des données

- Les préoccupations autour des mesures de protection des données sont généralisées. Le moindre doute place les organisations dans une position vulnérable
- Toutes les organisations (ou presque) rencontrent des défis en matière de protection des données. Bon nombre d'entre elles ont également subi des interruptions significatives au cours des douze derniers mois en raison de pertes de données et/ou d'interruptions de service des systèmes non planifiées
- Les menaces en matière de sécurité externes constituent les causes les plus fréquentes à l'origine des pertes de données et/ou des interruptions de service des systèmes non planifiées au cours des douze derniers mois
- Malgré les défis et les préoccupations liés à la protection des données, peu d'entre elles ont entièrement déployé un modèle de sécurité Zero-Trust

La menace grandissante des cyberattaques

- Le nombre d'organisations ayant subi une cyberattaque ou un incident au cours des douze derniers mois a augmenté, avec un coût moyen de 1,92 million de $ pour les entreprises
- De nombreuses organisations craignent que leurs données de sauvegarde soient infectées ou corrompues du fait d'attaques par ransomware
- À ce risque vient s'ajouter un excès de confiance autour des conséquences d'une attaque par ransomware
- Même si les polices d'assurance contre les ransomwares sont monnaie courante, elles font l'objet de nombreuses réserves, et rendent les organisations vulnérables sur le plan financier

L'utilisation du multicloud

- Même si le Cloud public reste un choix très prisé pour la mise à jour et le déploiement de nouvelles applications, la sécurité des données pose problème
- Face aux préoccupations en matière de sécurité, de nombreuses organisations migrent (ou ont prévu de migrer) une partie de leurs charges applicatives du Cloud public sur site
- Face à l'intensification des cyberincidents et à la confiance érodée dans les stratégies de protection des données, bon nombre d'entre elles considèrent la sécurité comme une composante essentielle des opérations hybrides multiclouds

La sécurisation d'un environnement Cloud

- À l'heure actuelle, les organisations utilisent plusieurs outils et solutions de sauvegarde pour protéger leurs charges applicatives, mais reconnaissent que certaines mises à niveau sont nécessaires
- Les organisations dépendent de plus en plus des prestataires de services Cloud pour protéger leurs charges applicatives dans les environnements Cloud

DELL Technologies