# Global Data Protection Index 2021

Principales conclusions – Juillet 2021

VansonBourne

DELL Technologies

# Portée des principales conclusions

1

L’environnement des risques en matière de protection des données

2

La menace représentée par les cyberattaques

3

Suivre le rythme des technologies nouvelles et émergentes

4

Les failles de sécurité en matière de protection des données dans les environnements Cloud

5

La croissance du « as-a-service »

6

Simplifier la protection des données

# Cinq points clés à retenir

De plus en plus adopté, le travail à domicile a **augmenté les risques en matière de protection des données et d'informatique**

**Beaucoup de professionnels sont peu convaincus de la capacité de leur organisation à protéger suffisamment les données** pour se défendre efficacement contre les cybermenaces et restaurer les données

Les investissements continus dans les technologies émergentes et le Cloud **peuvent multiplier les défis en matière de protection des données**

Beaucoup de professionnels souhaitent **exploiter le as-a-service** pour accroître la simplicité et la flexibilité de la protection des données

Certaines expériences montrent que la collaboration avec **moins de fournisseurs de protection des données** entraîne **de meilleurs résultats en la matière**

# Qui avons-nous interrogé ?

1 000 décideurs informatiques ont été interrogés en février, mars et avril 2021

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

Organisations de plus de 250 collaborateurs

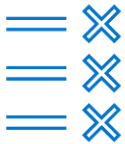
4 zones géographiques :

Amériques (200)
EMEA (450)
APJ (250)
Chine (100)

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

# Les décideurs informatiques sont peu convaincus de la capacité de leur organisation à satisfaire les SLO de récupération

# En outre, peu de professionnels pensent que les fonctionnalités de protection des données sont à la hauteur des normes internes et externes. Encore plus inquiétant, deux tiers des personnes interrogées pensent qu'elles vont subir un événement d'interruption au cours de l'année prochaine



58 %

ne sont pas très convaincus que leur entreprise **atteint ses objectifs de niveau de service de sauvegarde et restauration**

63 %

ne sont pas très convaincus que l'infrastructure et les processus actuels de protection des données de leur organisation sont **conformes aux réglementations de leur zone géographique en matière de gouvernance des données**

64 %

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

# À ces inquiétudes s’ajoutent les problèmes de perte de données et d’interruption de service des systèmes, qui continuent d’avoir un impact financier important sur les organisations

**959 493$**

Coût moyen de la perte de données au cours des 12 derniers mois (en USD)

**513 067$**

Coût moyen de l’interruption de service non planifiée des systèmes au cours des 12 derniers mois (en USD)

# 2. La menace représentée par les cyberattaques

# Les organisations ne sont pas convaincues que leurs mesures de protection des données puissent atténuer les effets des cyberattaques. De plus, la plupart d'entre elles pensent que le travail à domicile des collaborateurs augmente l'exposition

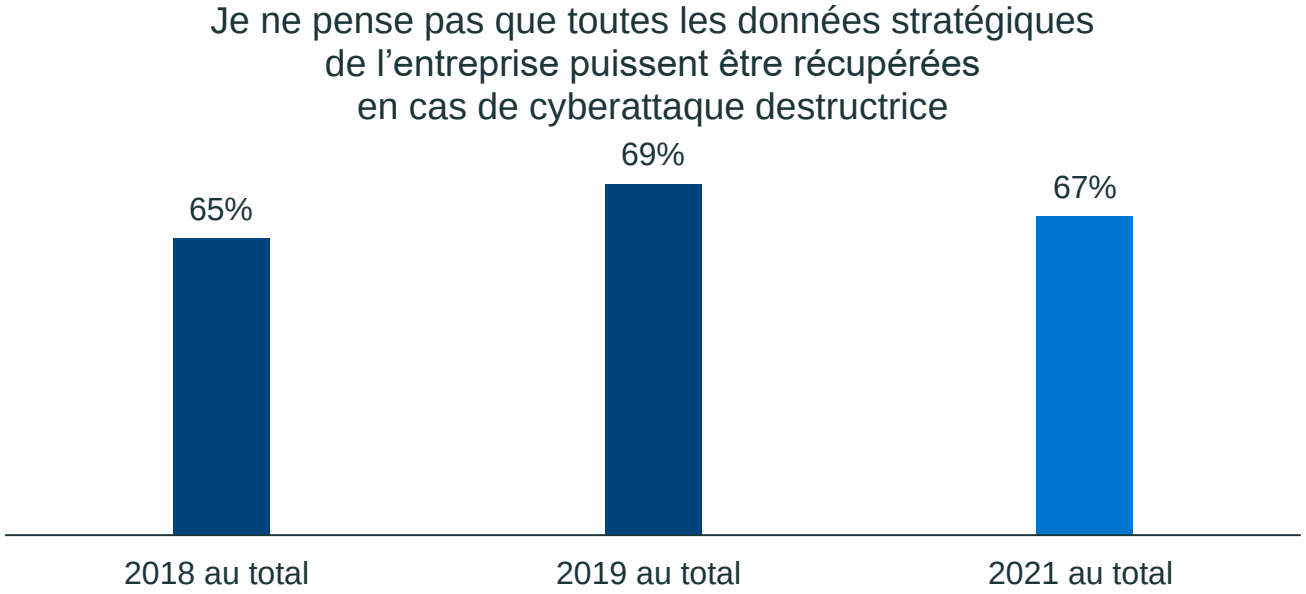
## 62 %

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

## 74 %

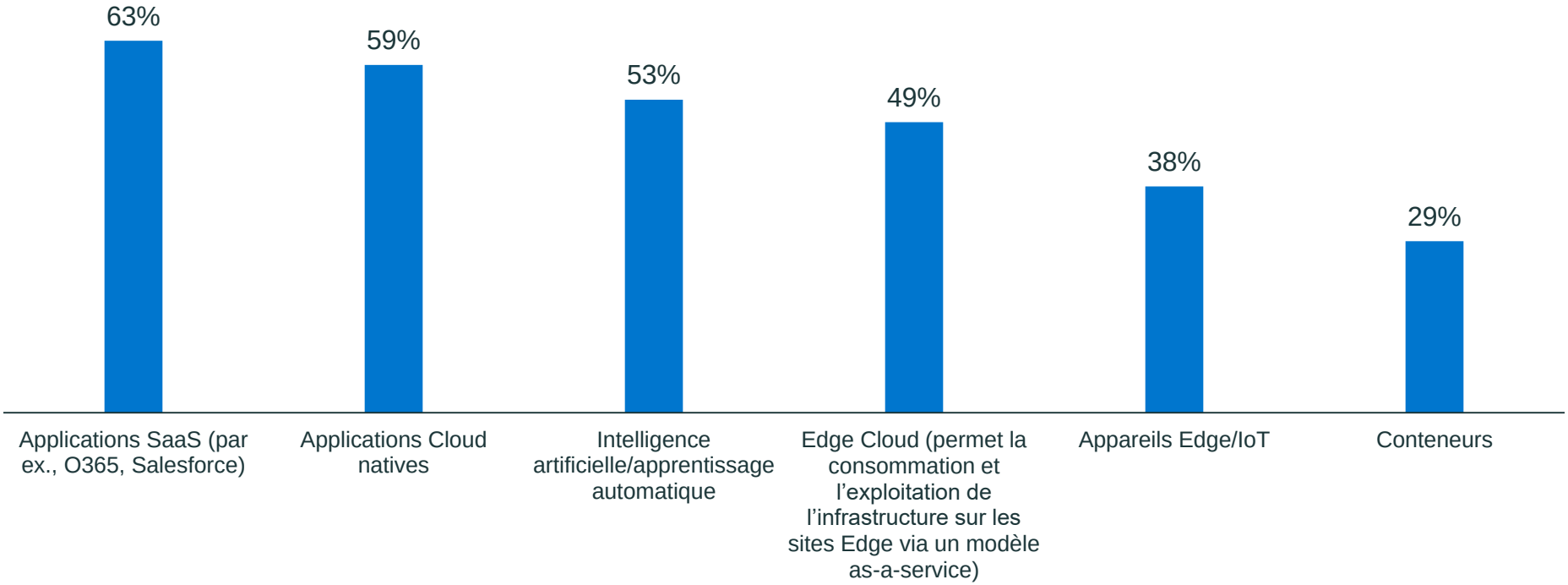
s'accordent à dire que leur organisation est **plus exposée à la perte de données** due aux cybermenaces depuis la tendance croissante **du travail à domicile**

# La capacité des organisations à faire face aux logiciels malveillants et aux menaces de ransomware suscite de nombreuses inquiétudes, car celles-ci ne sont pas certaines de pouvoir récupérer toutes les données stratégiques de l'entreprise en cas de cyberattaque destructrice

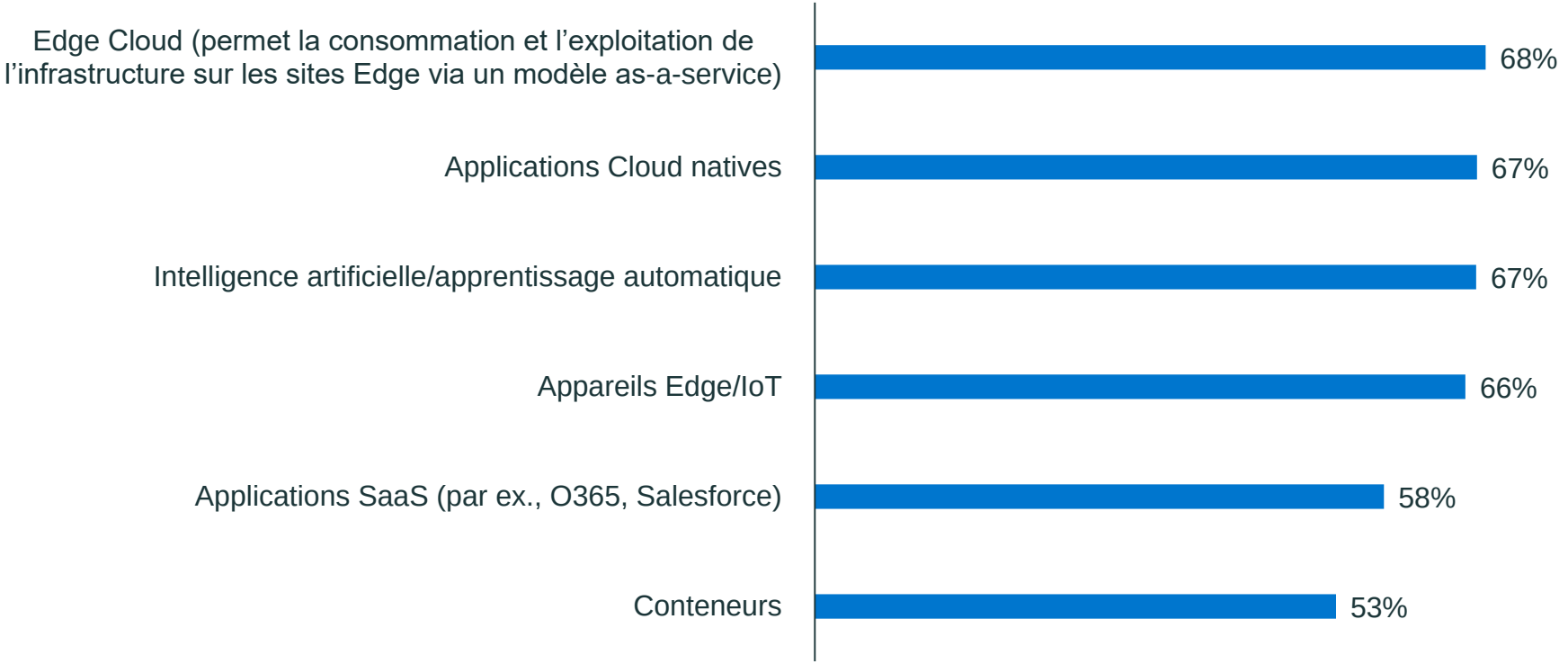


# 3. Suivre le rythme des technologies nouvelles et émergentes

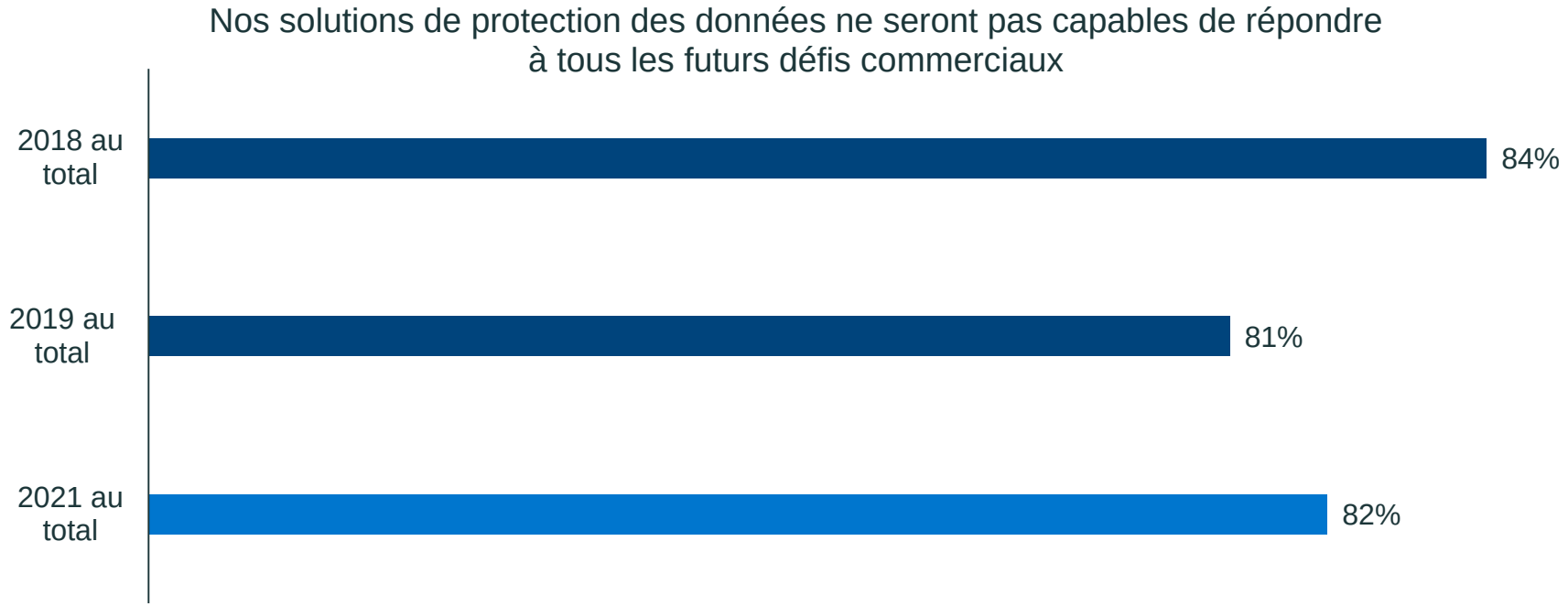
# Les organisations investissent dans de nombreuses nouvelles technologies, ce qui pourrait compliquer leurs défis en matière de protection des données



# Et c’est le cas de nombreuses organisations qui ont du mal à protéger ces technologies



# La difficulté à protéger les nouvelles technologies et les technologies émergentes contribue probablement au scepticisme vis-à-vis de la capacité des solutions de protection des données à répondre aux défis de demain



# Beaucoup d’organisations considèrent les technologies émergentes comme un risque pour la protection des données, et les inquiétudes par rapport aux événements d’interruption futurs sont élevées, en particulier chez les utilisateurs de plusieurs fournisseurs de protection des données

Les technologies émergentes (comme l’IA, l’IoT, la périphérie) présentent un risque pour la protection des données

Utilisation d’un seul fournisseur de protection des données

57 %

Utilisation de plusieurs fournisseurs de protection des données

64 %

Je crains que nous subissions un événement d’interruption (par exemple, perte de données, interruption de service des systèmes, etc.) au cours des 12 prochains mois

Utilisation d’un seul fournisseur de protection des données

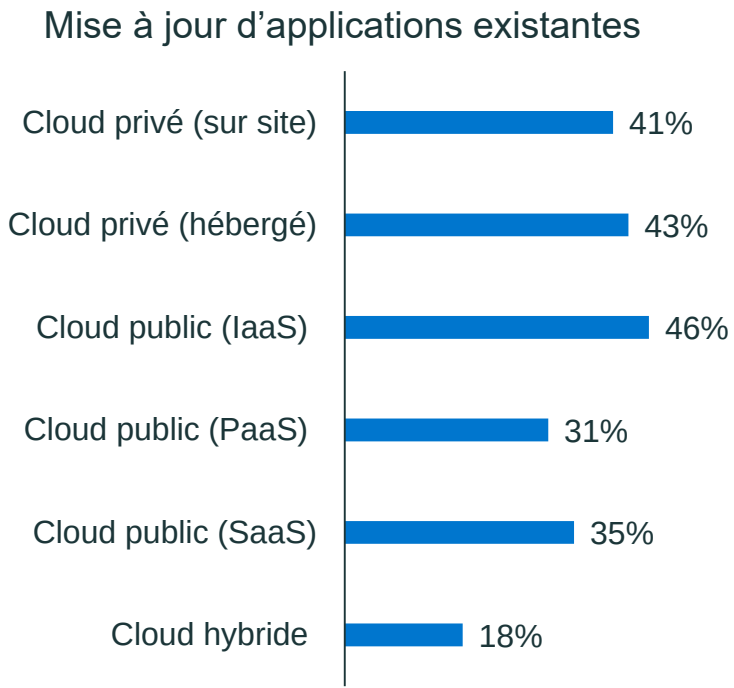
54 %

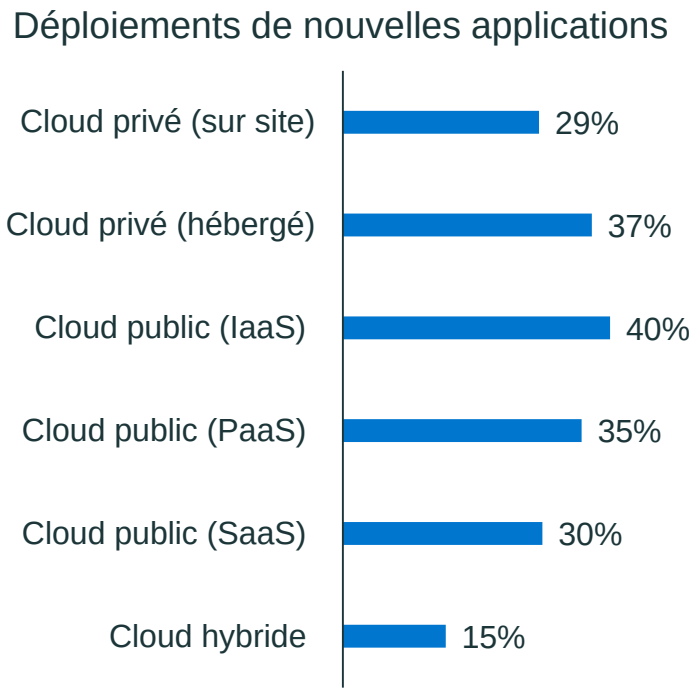
Utilisation de plusieurs fournisseurs de protection des données

68 %

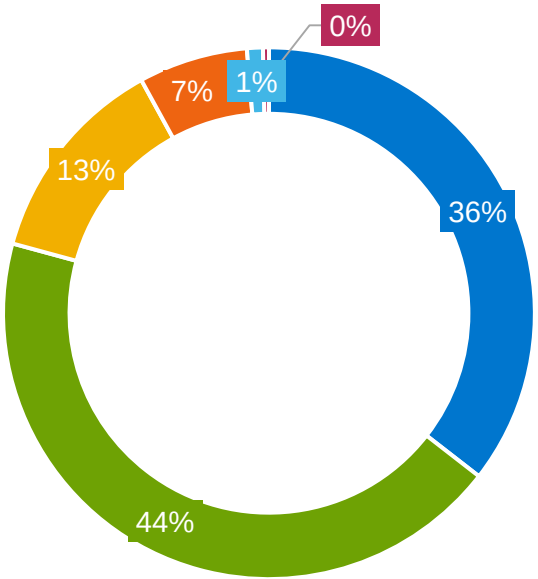
# 4. Les failles de sécurité en matière de protection des données dans les environnements Cloud

# Les applications sont mises à jour et déployées dans une vaste gamme d'environnements dans les infrastructures IT des organisations



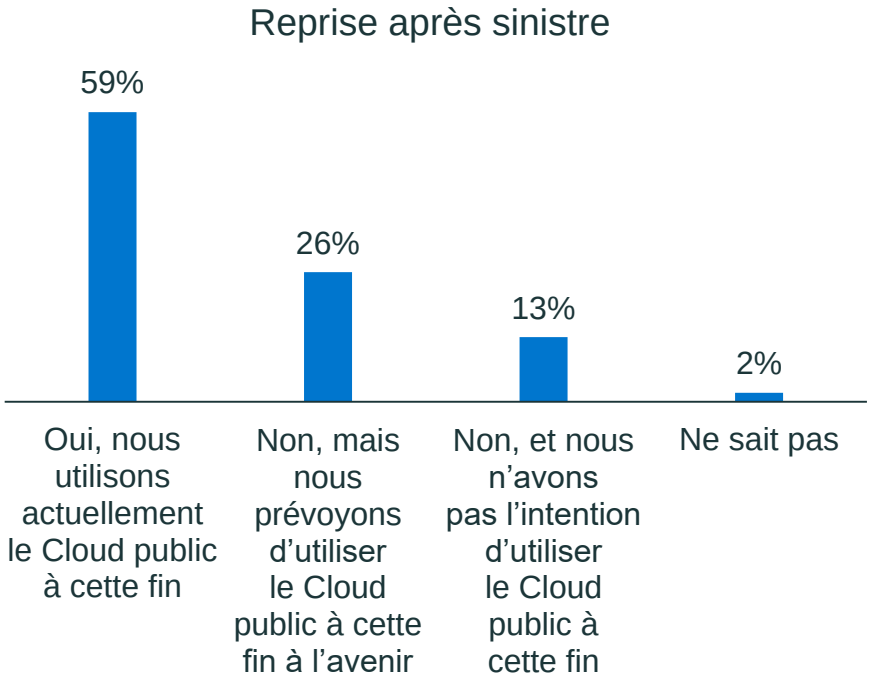



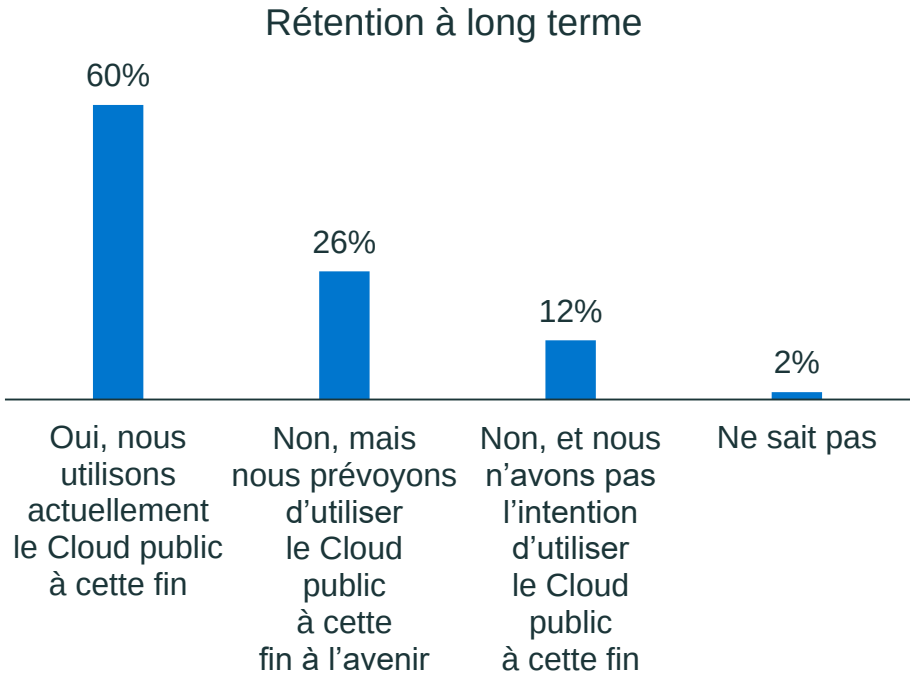
# Cependant, beaucoup manquent de confiance lorsqu'il s'agit de savoir comment protéger leurs données dans les environnements Cloud public




- Très confiants : nous protégeons toutes nos données sur le Cloud public
- Modérément confiants : nous protégeons toutes nos données stratégiques sur le Cloud public, mais pas l'ensemble de nos données
- Émettent des doutes : nous protégeons la plupart de nos données stratégiques sur le Cloud public
- Pas très confiants : nous protégeons certaines de nos données stratégiques sur le Cloud public
- Pas du tout confiants : nous ne protégeons pas nos données sur le Cloud public
- Ne sait pas

# Le Cloud public joue un rôle de plus en plus important dans les stratégies de reprise après sinistre et de rétention à long terme des organisations

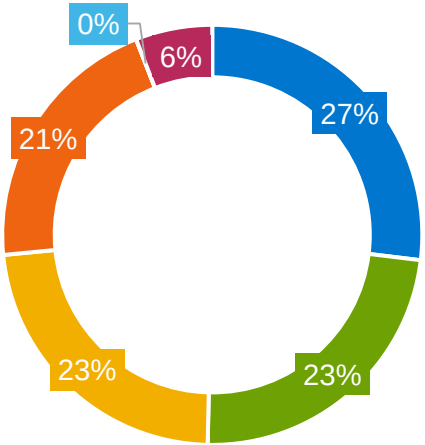


# Un certain nombre d’organisations utilisant plusieurs environnements Cloud n’utilisent pas de solutions spécifiques pour les protéger

**21 %**

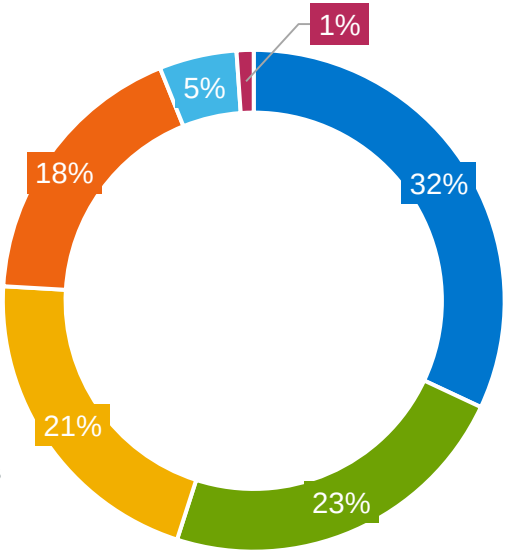
des professionnels pensent que lorsqu’ils utilisent plusieurs environnements Cloud, **chaque prestataire de services Cloud** est responsable de **la protection de leurs charges applicatives**




- Nous prévoyons de mettre à niveau notre solution de protection des données pour permettre la sauvegarde des charges applicatives sur plusieurs Clouds
- Notre solution de sauvegarde actuelle nous permet de protéger les charges applicatives exécutées dans plusieurs Clouds
- Nous utilisons plusieurs outils de sauvegarde pour protéger les charges applicatives exécutées dans plusieurs Clouds
- Chaque prestataire de services Cloud est responsable de la protection de nos charges applicatives
- Autre
- Nous n’exécutons pas de charges applicatives dans plusieurs environnements Cloud

# Il en va de même pour la protection des charges applicatives virtualisées à l'aide de VMware dans le Cloud

- Nous prévoyons de mettre à niveau notre solution de protection des données pour pouvoir sauvegarder leurs charges applicatives VMware dans le Cloud hybride
- Notre prestataire de services Cloud est responsable de la protection de nos charges applicatives
- Avec les outils de sauvegarde que nous utilisons et exploitons actuellement sur site
- Avec les outils de sauvegarde disponibles auprès des prestataires de services Cloud
- Nous n'exécutons ni ne prévoyons d'exécuter des charges applicatives virtualisées à l'aide de VMware dans le Cloud
- Ne sait pas

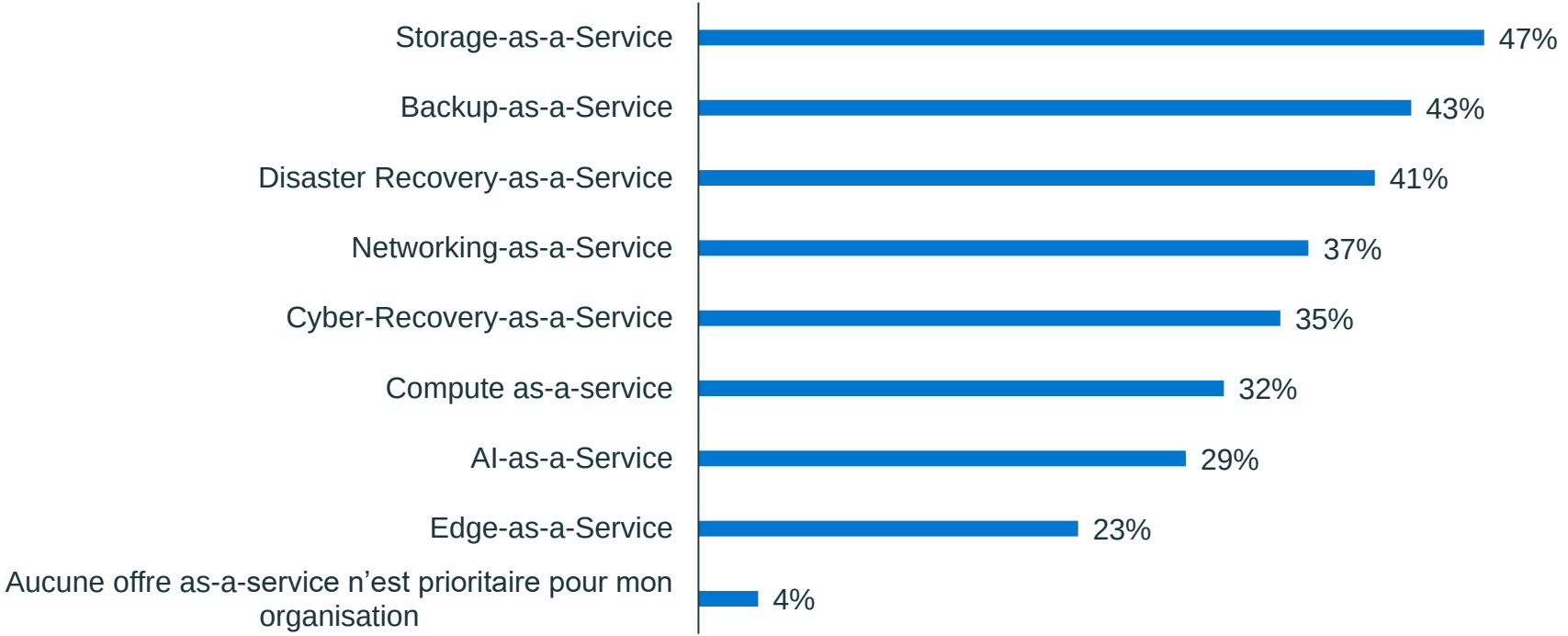



**23 %**

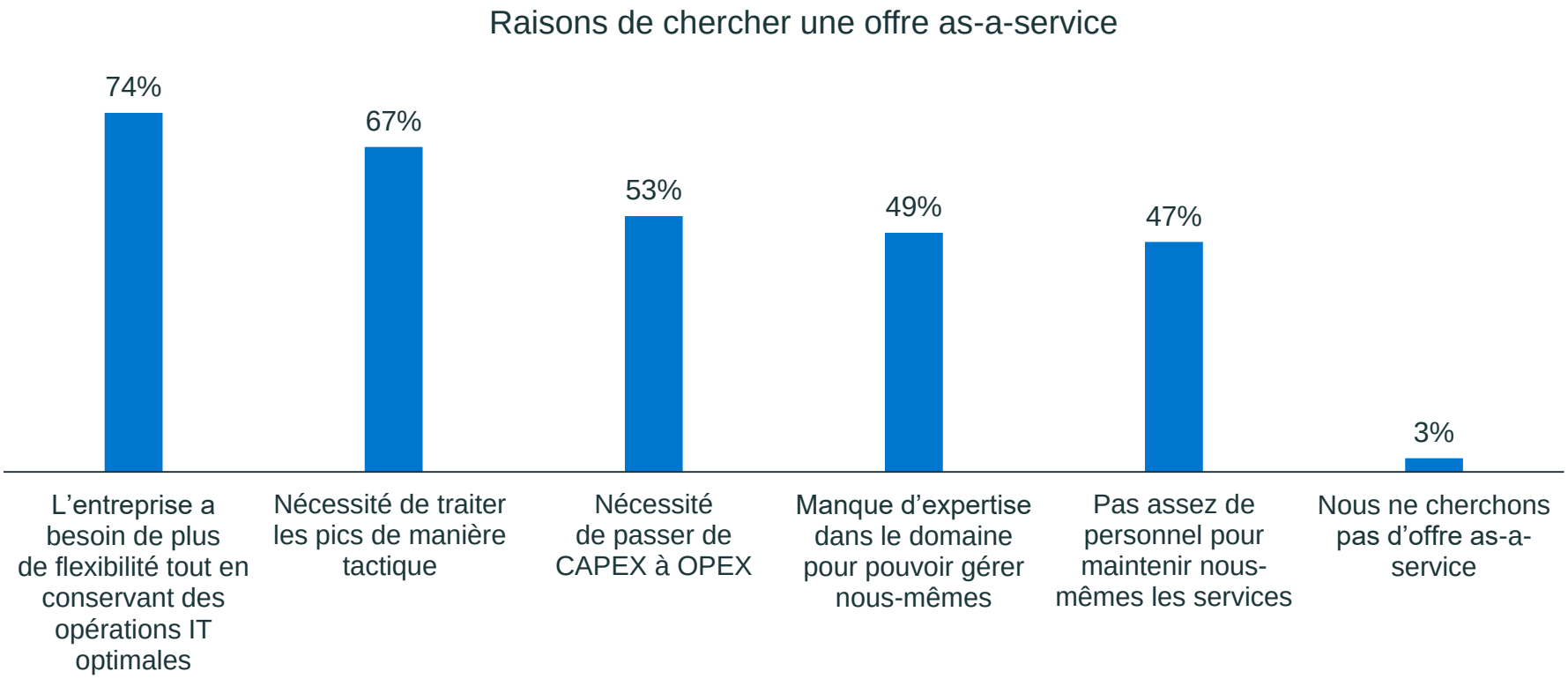
des professionnels pensent que leur **prestataire de services Cloud** est responsable de **la protection de leurs charges applicatives virtualisées**

# 5.La croissance du « as-a-service »

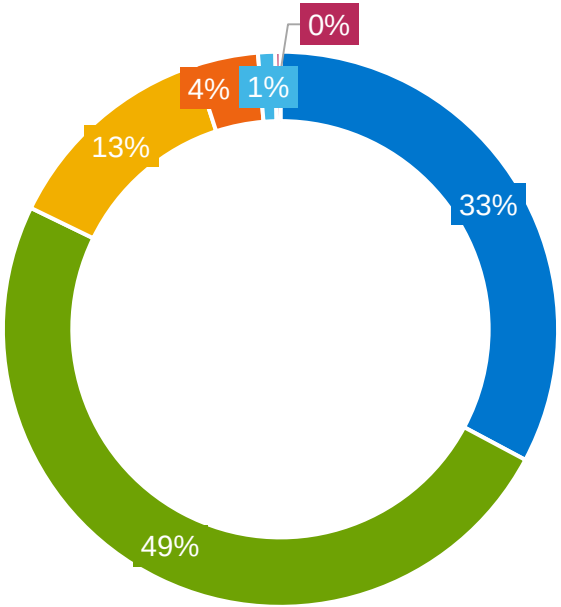
# La plupart des organisations donnent la priorité aux offres as-a-service, en particulier le Backup as-a-service et le Recovery as-a-service



# La popularité des offres as-a-service tient souvent à leur flexibilité



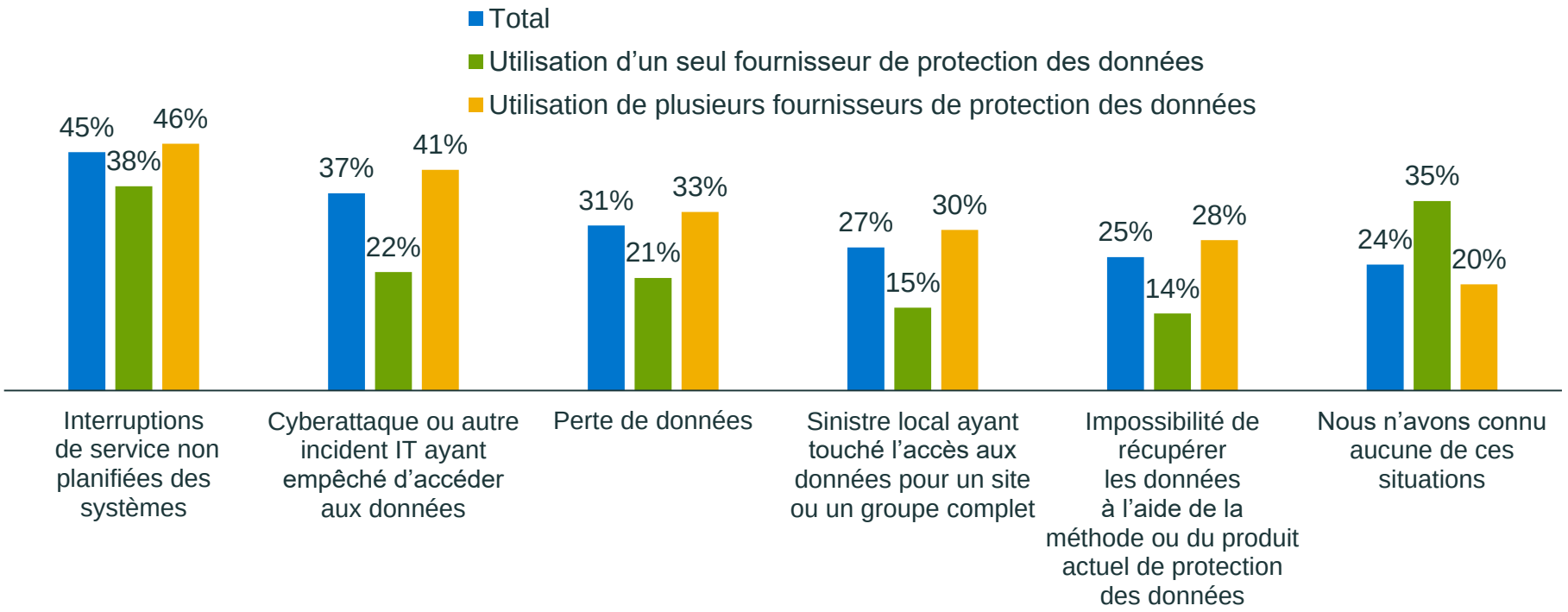
# La grande majorité des organisations préférerait travailler avec un fournisseur qui propose plusieurs offres as-a-service, ce qui suggère une volonté de consolider leurs charges applicatives avec moins de fournisseurs



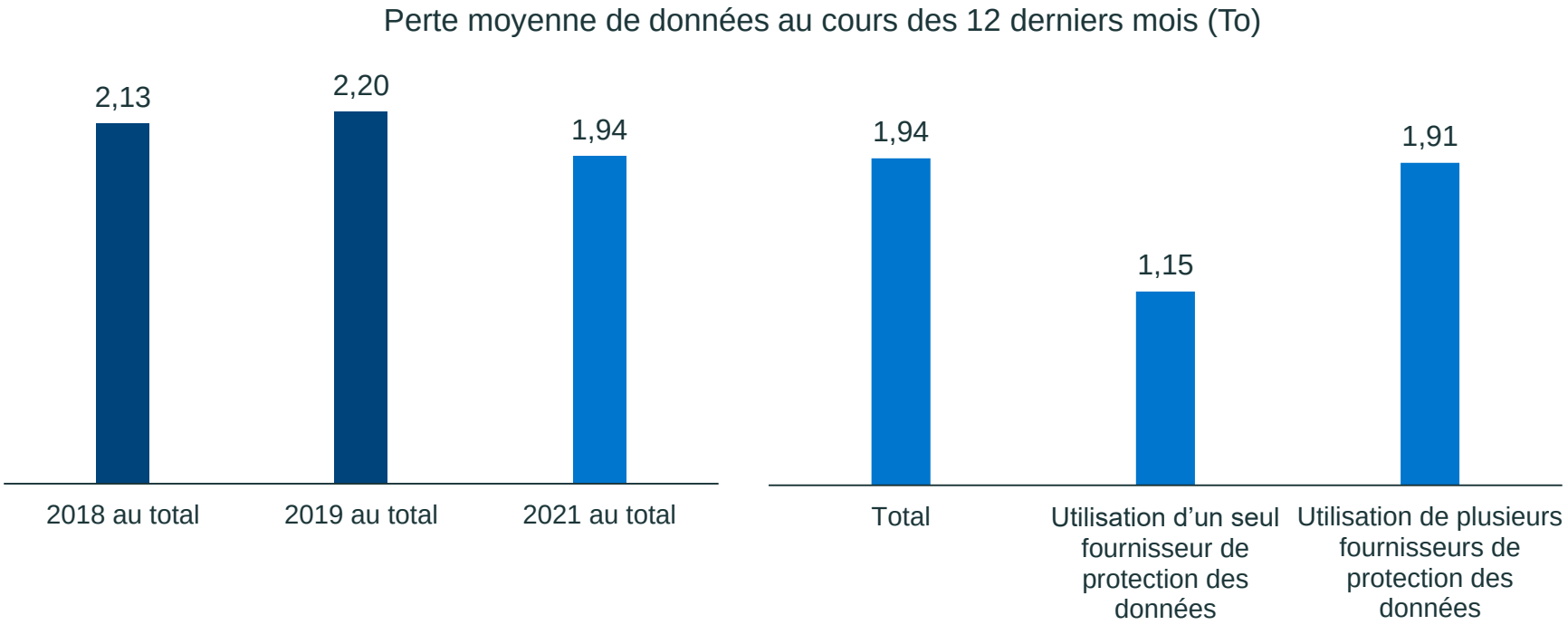

- Nous sommes beaucoup plus susceptibles de chercher un fournisseur qui propose plusieurs offres as-a-service
- Nous sommes un peu plus susceptibles de chercher un fournisseur qui propose plusieurs offres as-a-service
- Je suis indifférent quant à savoir si un fournisseur dispose de plusieurs offres as-a-service
- Nous sommes un peu moins susceptibles de chercher un fournisseur qui propose plusieurs offres as-a-service
- Nous sommes beaucoup moins susceptibles de chercher un fournisseur qui propose plusieurs offres as-a-service
- Ne sait pas

# 6. Simplifier la protection des données

# Les organisations utilisant plusieurs fournisseurs de protection des données sont plus susceptibles d'avoir subi des problèmes liés à la perte de données, à l'accès aux données ou aux interruptions de service des systèmes au cours de l'année passée que celles qui utilisent un seul fournisseur



# Et les organisations qui utilisent plusieurs fournisseurs de protection des données perdent en moyenne plus de données que celles qui utilisent un seul fournisseur



# Principales conclusions – en résumé (1/2)

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

- Beaucoup de professionnels craignent ne pas être capables de restaurer tous les systèmes/données pour répondre aux SLO en cas d’incident de perte de données
- Ils sont de plus en plus nombreux à craindre que les organisations subissent un événement d’interruption dans les douze prochains mois et que les impacts de ces événements puissent être dévastateurs sur le plan financier
- Les organisations doivent prendre des mesures pour s’assurer qu’elles sont prêtes à réagir à ces événements s’ils se produisent

### La menace représentée par les cyberattaques

- Les organisations craignent fortement de ne pas être en mesure de se protéger contre les logiciels malveillants et les menaces de ransomware, et la plupart d’entre elles s’accordent à dire que le risque de cyberattaques a augmenté avec l'accroissement du travail à distance
- Si les organisations sont forcément des cibles, peu d’entre elles sont convaincues de pouvoir restaurer toutes les données stratégiques de l’entreprise après une attaque

### Suivre le rythme des technologies nouvelles et émergentes

- Les organisations investissent dans une gamme de technologies nouvelles et émergentes, y compris les applications SaaS, l’IA/la ML et les appareils Edge/IoT, mais ont souvent du mal à garantir la protection de leurs données
- Beaucoup estiment que ces technologies représentent un risque pour la protection des données et que ces risques alimentent probablement la crainte que les organisations ne soient pas prêtes pour l’avenir et qu’elles risquent des interruptions au cours des douze prochains mois
- Les investissements dans les technologies émergentes sont une bonne chose et doivent être encouragés, mais les organisations doivent s’assurer que leur infrastructure de protection des données prend en charge ces technologies

# Principales conclusions – en résumé (2/2)

### Les failles de sécurité en matière de protection des données dans les environnements Cloud

- Les applications sont en cours de mise à jour et de déploiement dans une large gamme d'environnements Cloud, mais la confiance manque souvent en matière de protection des données
- Le Cloud joue un rôle important dans les stratégies de reprise après sinistre et de rétention à long terme
- Les organisations doivent s'assurer qu'elles disposent de solutions spécifiques pour protéger les données dans les charges applicatives multicloud et virtualisées, car certaines d'entre elles estiment que leurs fournisseurs de Cloud en sont responsables

### La croissance du « as-a-service »

- Les solutions as-a-service intéressent la plupart des organisations et feront probablement partie des solutions de protection des données de nombreuses entreprises à l'avenir. Cet intérêt s'explique souvent par la flexibilité de ces solutions
- La plupart d'entre elles préfèrent utiliser les solutions as-a-service proposées par des fournisseurs disposant de plusieurs offres, un choix qui pourrait contribuer à simplifier la protection des données pour ces organisations

### Simplifier la protection des données

- Les organisations qui utilisent un seul fournisseur de protection des données sont moins susceptibles d'avoir subi des pertes de données, des problèmes d'accès aux données et des interruptions de service non planifiées au cours de l'année passée que celles qui utilisent plusieurs fournisseurs
- Les utilisateurs d'un seul fournisseur ont également perdu moins de données que ceux utilisant plusieurs solutions, en moyenne
- Bien que les organisations soient tentées d'étendre leurs fonctionnalités de protection des données en investissant dans de nouvelles solutions, grâce à la consolidation de leurs solutions auprès d'un seul fournisseur, elles sont susceptibles d'être mieux protégées contre la perte de données et les interruptions de service

# Réduisez les risques et prenez une longueur d’avance

Le point de vue de Dell Technologies

Effectuer des examens réguliers de la préparation à la protection des données

Faire de la cyber-résilience une priorité

Consolider les initiatives de protection des données avec Dell

Rendez-vous sur DellTechnologies.com/GDPI pour en savoir plus


DELL Technologies