VERITAS

# Gérer les principaux problèmes du cloud

*Les stratégies cloud ne cessent de se compliquer.*

À mesure que les entreprises migrent leurs ressources vers le cloud, beaucoup se rendent compte qu'un stockage mal géré peut entraîner des coûts importants. Bien que le cloud offre de nombreux avantages, il crée également de nouveaux défis dans des domaines critiques tels que la sécurité, l'incertitude, le coût et la complexité.

**94 %** *des entreprises ont aujourd'hui une stratégie multi-cloud*[1]

**85 %** *des entreprises donneront la priorité au cloud d'ici 2025*[2]

## Défi n° 1

### La cybersécurité est complexe

*En 2021, les ransomwares ont coûté aux entreprises* **20 milliards de dollars**

*Les ransomwares et autres formes de malwares constituent un énorme problème, et ils se multiplient.*

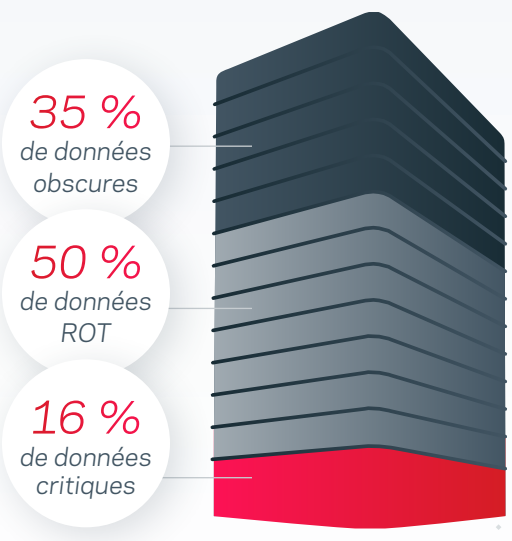
- Au cours du premier semestre 2022, on a recensé 2,8 milliards d'attaques de malwares. Cela représente une augmentation de 11 % par rapport aux six mois précédents.[3]
  Résultat : les vulnérabilités et les coûts montent également en flèche.
- Le coût moyen d'une attaque était de 1,85 million de dollars en 2021.[4]
- Veritas a constaté que 77 % des dirigeants d'entreprise et des responsables informatiques sont surpris par les dépenses qu'ils ont consacrées à la gestion des données et aux outils de cybersécurité.[1]
- Les défaillances en matière de cybersécurité sont coûteuses et peuvent entraîner des pertes de revenus, des amendes, des frais juridiques et des dommages à l'image de marque et à la réputation.

## Défi n° 2

### L'incertitude, les données obscures et le manque de visibilité constituent un danger

*La visibilité des données, de la périphérie au cœur et au cloud, est essentielle à la protection et à la résilience des données.*

- La plupart des responsables informatiques ne sont pas en mesure de suivre l'ensemble de l'empreinte des données de leur organisation, ce qui rend plus difficile la protection de toutes leurs données, la détection des menaces potentielles telles que les malwares et l'optimisation des coûts et de la complexité.
- Selon une étude de Veritas, les personnes interrogées manquent de clarté sur leurs données. En moyenne, les données de leurs organisations sont composées de 35 % de données obscures, de 50 % de données redondantes, obsolètes ou triviales (ROT) et de seulement 16 % de données critiques.[5]




## Défi n° 3

### Les coûts peuvent se multiplier

**50 %** *d'augmentation des coûts de stockage des données*

*À mesure que les exigences de stockage de données augmentent, les coûts augmentent.*

- Les solutions de stockage de données existantes n'optimisent pas l'utilisation, ce qui entraîne l'accumulation de données en double et inutiles à plusieurs endroits.
- Les coûts de stockage des données n'ont cessé d'augmenter ces dernières années. L'entreprise McKinsey & Co., experts en conseil en stratégie à l'échelle internationale, rapporte qu'ils ont augmenté de 50 % au cours des 5 dernières années.[6]
- En dédupliquant et en compressant les données, puis en les stockant sur un niveau de stockage moins cher, les entreprises peuvent réaliser des économies de stockage allant jusqu'à 99 % par rapport aux instantanés natifs du cloud.[7]

## Défi n° 4

### La complexité devient le paramètre par défaut

*L'accumulation d'outils, de technologies et de ressources implique l'introduction des niveaux supplémentaires d'administration et de gestion informatiques cloisonnées.*

- Bien que les outils cloud natifs puissent être rapides à activer, ils ne peuvent pas gérer les données dans des cadres multicloud, ce qui entraîne des outils plus disparates et une complexité opérationnelle.
- Pour maîtriser la complexité, les entreprises doivent adopter des solutions qui prennent en charge et rationalisent la gestion unifiée des données complexes, améliorent la protection et la sécurité des données et prennent en charge une architecture cloud native élastique et évolutive.

**45 %** *des applications sont réparties sur plusieurs clouds*

**83 %** *des organisations n'ont pas les ressources et l'expertise nécessaires pour les gérer correctement*[8]

## Défi n° 5

### Le cloud nécessite toujours une grande quantité de surveillance manuelle

*L'automatisation est essentielle pour éliminer les erreurs manuelles courantes et coûteuses. Sa valeur est particulièrement évidente pour les principaux cas d'utilisation concernant :*

- La technologie de gestion autonome des données qui protège automatiquement et intelligemment les données tout en garantissant leur conformité, leur sécurité et l'optimisation des coûts.
- L'intelligence artificielle (IA), l'apprentissage automatique (ML) et d'autres fonctionnalités d'automatisation et de mise à l'échelle automatique qui prennent en charge une architecture cloud native évolutive et élastique.
- Les appliances, les conteneurs et les microservices qui optimisent les capacités des infrastructures natives du cloud.

*Confusion autour du modèle de responsabilité partagée.*

Le modèle de responsabilité partagée est entouré de beaucoup de confusion et d'ambiguïté entre les fournisseurs de services cloud et leurs clients. Beaucoup comprennent en théorie que les fournisseurs de services cloud sont responsables de la résilience du cloud et que le client est responsable de la résilience dans le cloud. Mais l'exécution de cette méthode peut encore être vague et laisse souvent les données et les applications sans protection et vulnérables.

Grâce à une plate-forme sophistiquée qui prend en charge les environnements multi-cloud modernes, Veritas permet un meilleur contrôle, une réduction des risques et une meilleure gestion des coûts, tout en veillant à ce que vous respectiez votre part du modèle de responsabilité partagée.

## Veritas change tout

*Veritas propose une technologie de nouvelle génération qui révolutionne la gestion des données, la résilience, la cybersécurité et la durabilité dans le cloud.*

*En savoir plus sur* ***www.veritas.com/fr/fr/solution/cloud-data-security***

VERITAS
+1 (866) 837 4827
2625 Augustine Drive, Santa Clara, CA 95054
www.veritas.com/fr/fr
Pour obtenir nos coordonnées dans le monde entier, rendez-vous sur :
veritas.com/fr/fr/company/contact

1. Veritas et Vanson Bourne, « The Vulnerability Lag ». https://www.veritas.com/content/dam/Veritas/docs/reports/GA_ENT_AR_Veritas-Vulnerability-Gap-Report-Global_V1414.pdf
2. Gartner, « Gartner Identifies Four Trends Driving Near-Tern Artificial Intelligence Innovation », 7 septembre 2021. https://www.gartner.com/en/newsroom/press-releases/2021-09-07-gartner-identifies-four-trends-driving-near-term-artificial-intelligence-innovation
3. SonicWall, « 2022 Cyber Threat Report ». https://www.sonicwall.com/2022-cyber-threat-report/
4. Cloudwards, « Ransomware Statistics, Trends and Facts for 2022 and Beyond », 22 mars 2022. https://www.cloudwards.net/ransomware-statistics/
5. Veritas et Vanson Bourne, « The Vulnerability Lag ». https://www.veritas.com/content/dam/Veritas/docs/reports/GA_ENT_AR_Veritas-Vulnerability-Gap-Report-Global_V1414.pdf
6. McKinsey, « Reducing data costs without jeopardizing growth », 31 juillet 2020. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/reducing-data-costs-without-jeopardizing-growth
7. Veritas, « Cloud-Optimized Backup from Snapshot and Autoscaling in NetBackup 10 ». https://www.veritas.com/content/dam/www/en_us/documents/technical-documents/TB_netbackup_cloud_optimized_backup_snapshot_V1510.pdf
8. Flexera, « 2022 State of the Cloud Report ». https://info.flexera.com/CM-REPORT-State-of-the-Cloud?lead_source=Website%20Visitor&id=Flexera.com-PR

Copyright © 2024 Veritas Technologies LLC. Tous droits réservés. Veritas, le logo Veritas, Veritas Alta, le logo Veritas Alta et NetBackup sont des marques commerciales ou des marques déposées de Veritas Technologies LLC ou de ses filiales aux États-Unis et dans d'autres pays. Les autres noms cités peuvent être des marques déposées appartenant à leurs propriétaires respectifs.

V1609 09/22