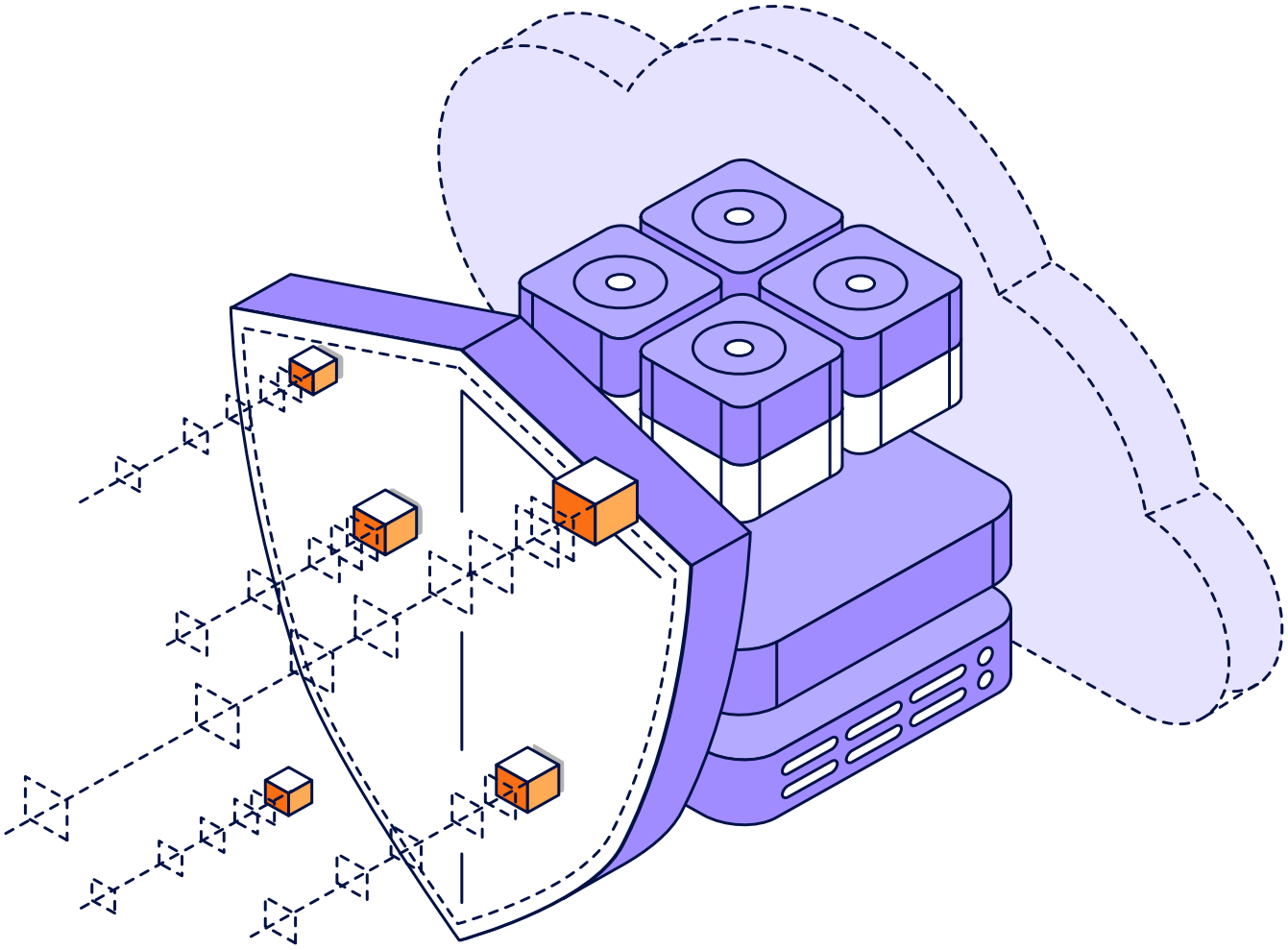
La cyber-résilience pour le cloud hybride

Retours d'expérience de plus de 7 000 professionnels de l'IT et de la sécurité



Ces dernières années ont été marquées par une évolution : du datacenter sur site vers ***le cloud lorsque cela s'impose***, vers des stratégies ***axées prioritairement sur le cloud***, vers le ***cloud hybride partout***, vers le stade où en sont la plupart des entreprises aujourd'hui dans l'adoption du ***multicloud stratégique*** comme mode normal de fourniture de services IT modernes. En 2024, les entreprises ne s'interrogent pas sur l'utilité des services basés sur le cloud ni sur ceux qu'elles doivent choisir. Elles se demandent plutôt combien de clouds il leur faut et comment leur équipe IT va tous les gérer, en assurant parallèlement la prévention de la cybersécurité, la protection des données et d'autres contrôles essentiels.

En réponse à ces questions, cette synthèse rassemble trois études indépendantes menées entre août 2022 et mars 2023 :

- **Tendances de la protection du cloud en 2023**
  Enquête auprès de 1 700 administrateurs IaaS, PaaS et SaaS au sujet de leurs stratégies de protection des données.
- **Rapport sur les tendances de la protection des données en 2023**
  Enquête auprès de 4 200 décideurs IT responsables de la stratégie de protection des données de leur entreprise.
- **Rapport sur les tendances des ransomwares en 2023**
  Enquête auprès de 1 200 RSSI et professionnels de la sécurité/sauvegarde d'une entreprise victime d'une cyberattaque en 2022.

Ces trois enquêtes ont été réalisées de manière impartiale par des bureaux d'études ou des cabinets d'analyses indépendants. Ces données acquises par Veeam® font l'objet de publications sous différentes formes. Cette synthèse met en évidence quatre tendances majeures :

- Les services basés sur le cloud sont essentiels pour protéger les datacenters et les workloads hébergés dans le cloud.
- Les clouds sont tout aussi exposés aux attaques par ransomware, voire plus.
- Protéger un cloud à l'aide d'un autre est une bonne idée, mais pas à l'aide de lui-même.
- Les équipes chargées de la sécurité, la DR (reprise après incident), le cloud et le site ne sont pas coordonnées : c'est la priorité !

Les services basés sur le cloud sont essentiels pour protéger les datacenters et les workloads hébergés dans le cloud

82 %

des entreprises utilisent désormais des stockages basés sur le cloud offrant une fonctionnalité d'inaltérabilité.

Les études révèlent systématiquement que les services basés sur le cloud sont indispensables pour protéger les workloads sur site traditionnels, comme ceux hébergés dans le cloud. *En particulier, les stockages basés sur le cloud permettent de disposer de* ***cibles pérennes*** *(grâce à l'inaltérabilité, par ex.) et d'une* ***infrastructure de DR*** *lorsqu'elle est nécessaire.*

Il existe deux vérités quasi universelles sur les ransomwares, que partagent la plupart des entreprises :

- Pour que les serveurs des datacenters soient protégés, les données doivent se trouver à l'extérieur de l'entreprise (hors site ou dans le cloud, par ex.).
- Pour se relever d'une attaque par ransomware, il faut disposer de copies de sauvegarde à l'abri des cybermenaces.

Le rapport sur les tendances des ransomwares en 2023 montre une association de ces deux postulats dans les « retours d'expérience » : **82 %** des entreprises utilisent désormais des stockages basés sur le cloud offrant une fonctionnalité d'inaltérabilité.[1]

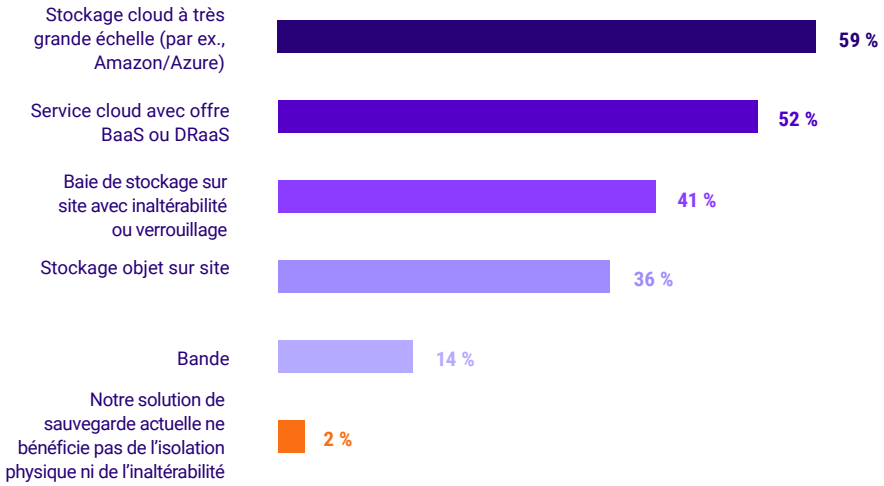


Figure 1.1

Votre entreprise dispose-t-elle de sauvegardes hors ligne, entièrement isolées ou inaltérables utilisant les systèmes suivants ?

Une fois assurée de disposer de copies de sauvegarde pérennes, l'entreprise peut aussi s'attacher à d'autres aspects de sa stratégie traditionnelle de continuité d'activité et reprise après incident (BC/DR). Les cyberattaques étant de plus en plus souvent perçues comme un sinistre (quoique spécial) parmi d'autres, il n'est pas étonnant que de nombreuses entreprises associent étroitement cyber-résilience et DR. Dans les deux cas, une question des plus pragmatiques vient ensuite : **vers où faut-il restaurer ou basculer ?**

Les retours d'expérience des victimes de cyberattaques montrent que les stratégies des entreprises pour rétablir l'activité incluent la capacité de restaurer les serveurs du datacenter vers une infrastructure hébergée dans le cloud pour effectuer la remédiation après l'attaque par un ransomware ou une autre crise.[2]

Figure 1.2

Lors de la restauration de serveurs après une attaque par ransomware, où restaurez-vous vos données ?

Comme illustré ci-dessus, la plupart des entreprises ont élaboré une stratégie hybride flexible, adaptée à l'ampleur de la crise. En réalité, elles sont **71 %** à pouvoir revenir à la normale grâce au cloud et **81 %** à s'appuyer sur une infrastructure locale : des solutions qui se recoupent largement (preuve de flexibilité). Les entreprises qui préparent leur PRA (plan de reprise d'activité) pour affronter toute sortes de crises sont **54 %** à prévoir de basculer vers un site de secours et **46 % à choisir une infrastructure hébergée dans le cloud comme site de DR**. Cela étant, il existe différents moyens de se doter d'un site de DR basé sur le cloud.[3]

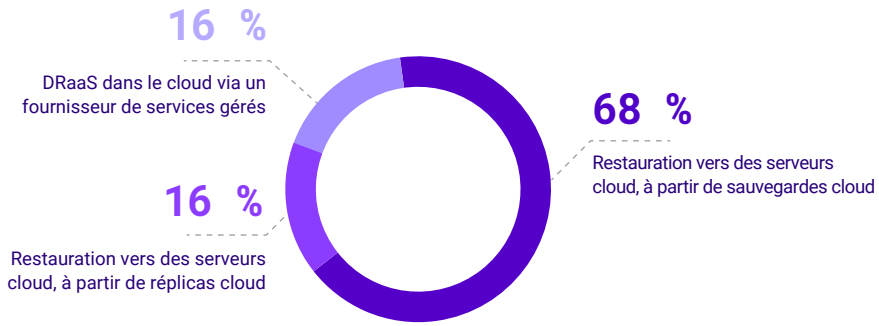


Figure 1.3

Lorsque vous utilisez des services cloud pour la reprise après incident, comment rétablissez-vous l'exploitation ?

Que votre PRA s'appuie sur un fournisseur de DR en mode service (DRaaS) ou sur une infrastructure autogérée hébergée dans le cloud, comme Amazon Web Services ou Microsoft Azure, son succès dépend d'au moins deux fonctionnalités stratégiques :

- La capacité de transformer une sauvegarde pendant la restauration de sorte qu'un serveur de production physique ou virtuel à l'origine puisse être rétabli et démarré sur un hôte dans le cloud.
- La capacité d'orchestrer le processus de reprise, y compris la quarantaine nécessaire pour détecter les logiciels malveillants pendant le workflow de restauration.

Malheureusement, les entreprises sont seulement :

- **18 %** à être capables de programmer des scripts de workflows orchestrés pour la reprise avec basculement. [4]
- **44 %** à utiliser des zones de test isolées ou « sandbox » pour analyser les logiciels malveillants pendant la restauration, et s'assurer ainsi de ne pas réinfecter l'environnement.[5]

Ces points sont potentiellement difficiles à traiter pour la direction : la solution ou le service de protection des données de l'entreprise peut-il automatiser la restauration à grande échelle et/ou garantir une restauration sûre ?

Les clouds sont tout aussi exposés aux attaques par ransomware, voire plus

Probablement parce que les services basés sur le cloud sont facilement accessibles au sein des architectures IT hybrides, les études révèlent systématiquement que **les workloads cloud sont tout aussi susceptibles d'être ciblés pendant une cyberattaque**. *En réalité, comme de nombreuses entreprises doivent recourir à différentes technologies de sécurité pour empêcher l'accès aux services cloud, par comparaison avec les ressources de leur datacenter, cela crée de nouvelles opportunités d'attaque, notamment en perturbant la connectivité entre les utilisateurs et leurs plateformes cloud.*

Malgré le constat que le cloud n'appartient pas au futur, mais bien au présent, il faut aussi reconnaître que les équipes IT ne désactivent pas les plateformes sur site à un rythme équivalent à celui auquel les nouveaux workloads investissent les services basés sur le cloud. Les entreprises continuent d'adopter des infrastructures hébergées dans le cloud dans le cadre de leur stratégie toujours plus hybride de fourniture de services IT.

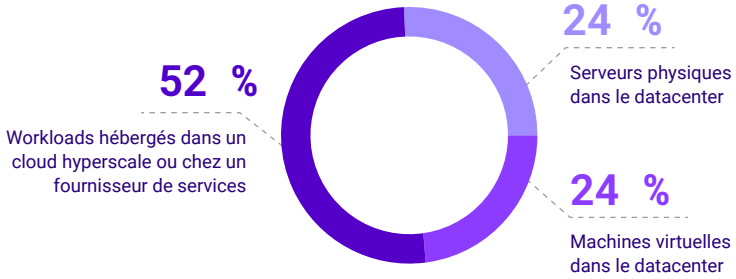


Figure 2.1

Distribution « hybride » des plateformes envisagée pour les workloads sur les serveurs de production en 2024.[6]

Il est à noter que, contrairement à l'évolution des plateformes au sein des services IT orientés datacenter, il n'y a pas simplement une architecture avec « un cloud » à déployer, utiliser et protéger, indépendamment du fournisseur de cloud. Au contraire, il faut envisager des architectures constituées de nombreux clouds proposés par divers fournisseurs, avec autant de cadres de gestion sous-jacents très différents les uns des autres.

Figure 2.2

Architectures constituées de nombreux clouds.

Malheureusement, bien qu'on associe souvent résilience et services basés sur le cloud, des pannes continuent de se produire. Leurs causes sont liées à des problèmes chez le fournisseur de services cloud, à des erreurs de configuration par l'administrateur et à la connectivité entre les utilisateurs et les services cloud eux-mêmes. Cela étant, les rapports de 2021 et 2022 révélaient que les pannes liées aux cyberattaques avaient augmenté d'une année sur l'autre et que leur impact restait le plus important (sans signe de ralentissement en 2023).[7]

- **48 %** des entreprises ont subi des interruptions de leur IT en raison d'une **indisponibilité des ressources du cloud public**.
- **52 %** des entreprises ont subi des interruptions de leur IT en raison de **pannes d'infrastructure ou de réseau**.
- **53 %** des entreprises ont subi des interruptions de leur IT en raison d'un **événement de cybersécurité**.

La plupart du temps, le premier point d'entrée d'une cyberattaque est opportuniste (spamming d'e-mails de phishing dans l'espoir qu'un utilisateur va cliquer), mais il s'ensuit un ciblage des systèmes s'appuyant sur des vulnérabilités identifiées ou des défaillances potentielles dans la sécurité des plateformes IT du marché. Le **rapport sur les tendances des ransomwares en 2023** révèle que **38 %** **des attaques ciblent des workloads hébergés dans le cloud**.[8]

Interrogés sur les quantités de données chiffrées/altérées pendant les cyberattaques dont ils ont été victimes, les 1 200 répondants ont indiqué qu'elles étaient quasiment réparties également entre le cloud et le site.

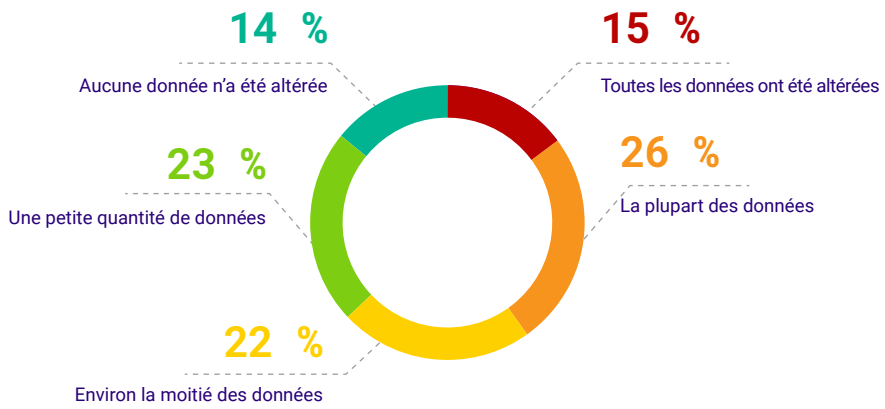


Figure 2.3

Pourcentage des données hébergées sur des plateformes cloud altérées lors de la dernière attaque par ransomware.[9]

Il est important de savoir que les taux d'infection des données sont équivalents dans les datacenters, les bureaux distants et succursales, et les clouds, avec deux vérités essentielles à la clé :

- La fluidité de fourniture des services IT hybrides est telle qu'une fois l'environnement de la victime menacé, les données hébergées dans le cloud sont aussi vulnérables en cas d'attaque que les applications et les fichiers présents dans le datacenter physique.
- La fluidité et l'égalité de vulnérabilité impose de protéger les fichiers, bases de données et applications hébergés dans le cloud, en employant la même rigueur et les mêmes méthodologies que pour les workloads sur site.

À l'horizon 2024, pour la première fois, on devrait compter plus de workloads exécutés à l'extérieur qu'à l'intérieur des datacenters physiques auto-gérés.

Protéger un cloud à l'aide d'un autre est une bonne idée, mais pas à l'aide de lui-même

2 contre 1

La protection des données relève en majorité de l'équipe de sauvegarde « traditionnelle » plutôt que des administrateurs cloud.

Sur la question de « qui » sauvegarde les données de leurs clouds et « comment » ces données sont protégées en 2023, les trois études confirment que ***l'équipe de sauvegarde principale (ou le fournisseur de services) qui protège le reste des données de l'entreprise sur site est aussi le plus souvent chargée de protéger les données hébergées dans le cloud.*** *Cela étant, une grande confusion règne toujours concernant le « comment ». C'est généralement le cas lorsque les entreprises supposent que l'utilitaire intégré dans leur plateforme est leur seule option, alors qu'il existe une solution de sauvegarde de niveau entreprise hétérogène.*

Avant de s'intéresser au « comment », il convient de prendre en considération les différents profils derrière le « qui » : à 2 contre 1, la protection des données est majoritairement l'affaire de l'équipe de sauvegarde IT « traditionnelle » plutôt que celle des administrateurs cloud.

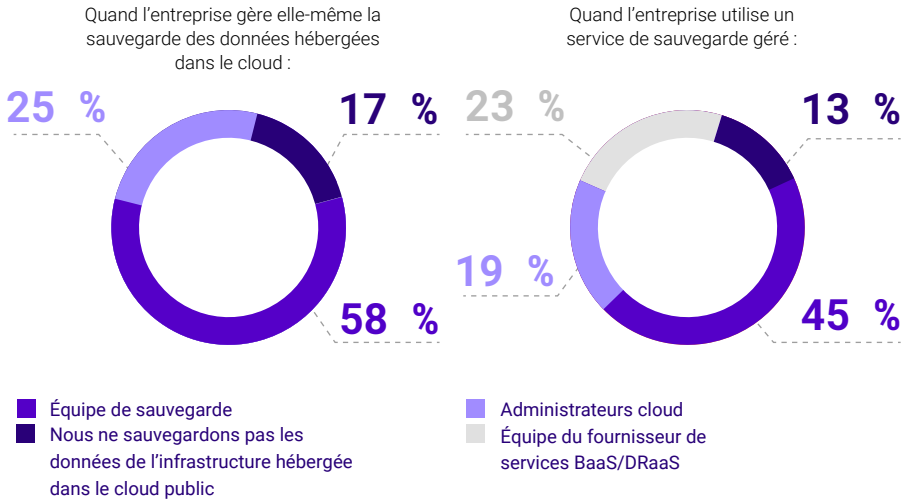


Figure 3.1

Qui gère la sauvegarde/protection des données sur les serveurs hébergés dans le cloud ?[10]

Statistique surprenante : un répondant sur huit **(13 %)** pense que l'entreprise ne sauvegarde pas son infrastructure hébergée dans le cloud. Pour de nombreuses entreprises qui adoptent une stratégie hybride, la question suivante concerne l'emplacement des sauvegardes du cloud, qui peuvent se trouver sur le même cloud, dans une autre région, sur un autre cloud, voire sur site.
Cet aspect revêt une grande importance au moment de choisir comment sauvegarder les workloads hébergés dans le cloud :

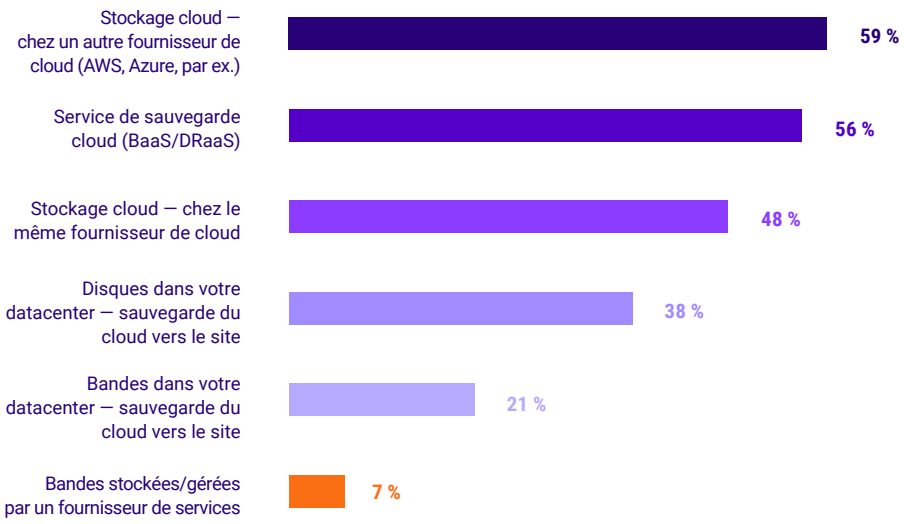


Figure 3.2

Où votre entreprise stocke-t-elle les sauvegardes de ses données cloud qu'elle doit conserver au minimum pendant un an ?[11]

- **37 %** des décideurs IT considèrent que la capacité de déplacer les workloads entre les clouds est caractéristique d'une solution de protection des données « moderne » ou « innovante ».[12]
- **88 %** des entreprises ont rapatrié des workloads du cloud vers leur site ou les ont déplacés vers un autre cloud.[13]

Bien sûr, il existe une autre possibilité de sauvegarder les workloads hébergés dans le cloud : s'en remettre simplement à l'utilitaire ou la fonction d'exportation qu'intègrent de nombreux fournisseurs de cloud pour chaque workload spécifique. Souvent, le facteur limitant est simplement la méconnaissance des outils tiers disponibles pour protéger

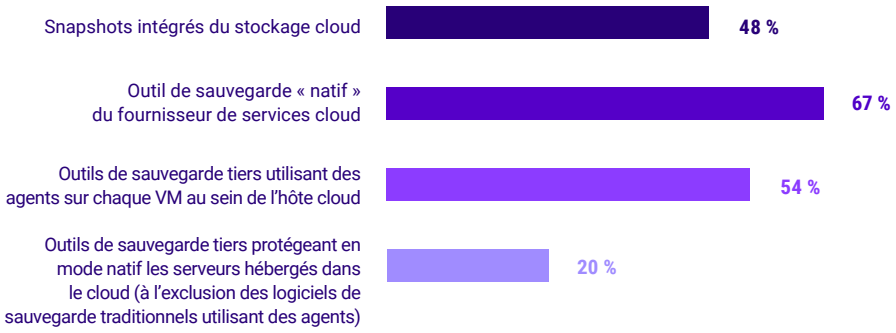


Figure 3.3

Quels mécanismes de protection des données hébergées dans le cloud connaissez-vous (que vous les utilisiez ou pas aujourd'hui) ?

totalement les workloads cloud.[14]

Si vous envisagez d'utiliser des snapshots, demandez-vous si vous pourriez dépendre exclusivement de ceux de vos serveurs de fichiers locaux. De fait, ce sont de puissants outils pour les points de restauration quasi actuels qui peuvent être instantanés. Toutefois, **les snapshots ne peuvent en aucun cas se substituer aux sauvegardes**, pour les raisons suivantes :

- Ils relèvent du même silo en termes d'exposition (ils font le lien entre un NAS autonome et une pile de stockage IaaS, notamment les informations d'identification communes).
- Leur rétention finit par être coûteuse. C'est pourquoi la plupart des entreprises ne les conservent que quelques jours, contre des semaines, des mois ou des années pour les sauvegardes.

Si vous envisagez de recourir à des utilitaires axés sur les workloads « natifs » ou intégrés, demandez-vous sur quoi repose la protection de vos plateformes sur site :

- ZDLRA (ou RMAN) pour les bases de données **Oracle ;**
- utilitaire de sauvegarde (ou outil système) de Windows NT pour les **serveurs Windows ;**
- VDPA pour les hôtes **VMware ;**
- ASB pour **Microsoft 365.**

Interrogez-vous maintenant sur le nombre d'outils de sauvegarde que votre équipe IT est prête à gérer et sur le budget que vous pouvez consacrer au stockage (sachant que ces outils produisent des cibles et des formats différents). Les utilitaires pour snapshots et autres plateformes uniques (intégrés, par ex.) sont encore plus problématiques, car ils sont généralement conçus pour une plage de rétention restreinte permettant des retours arrière rapides en cas d'erreur récente (des données écrasées ou une importation invalide, par exemple). Sachant qu'il est parfois nécessaire de se relever de l'attaque d'un ransomware resté dormant pendant des semaines, ces tactiques paraissent insuffisantes (ou trop onéreuses). Ce ressenti se mesure grâce à ces deux autres statistiques :

- **35 %** des décideurs IT considèrent que **standardiser la protection dans les stratégies locales et IaaS/SaaS** est caractéristique d'une solution de protection des données « moderne » ou « innovante ».[15]
- **42 %** des entreprises pensent que la **capacité de protéger les workloads cloud** est une caractéristique indispensable pour une solution de protection des données.[16] Ce ressenti a été à la fois le plus partagé et le plus important en 2023.

35 %

des décideurs IT considèrent que standardiser la protection dans les stratégies locales et IaaS/SaaS est caractéristique d'une solution de protection des données « moderne » ou « innovante ».

Les équipes chargées de la sécurité, la DR, le cloud et le site ne sont pas coordonnées : c'est la priorité !

Différents profils ont été interrogés dans le cadre de ces trois enquêtes : décideurs IT chargés de la protection des données, RSSI ou responsables équivalents, professionnels de la sécurité, administrateurs IaaS/PaaS/SaaS et opérateurs de sauvegarde. Les résultats montrent qu'aucune équipe n'est responsable à elle seule d'une fonction à part entière, les sphères d'influence et de responsabilité se chevauchant toujours. Pourtant, ***les réponses révèlent rarement une coordination, que ce soit sur les exigences stratégiques ou la mise en œuvre/l'utilisation des technologies.***

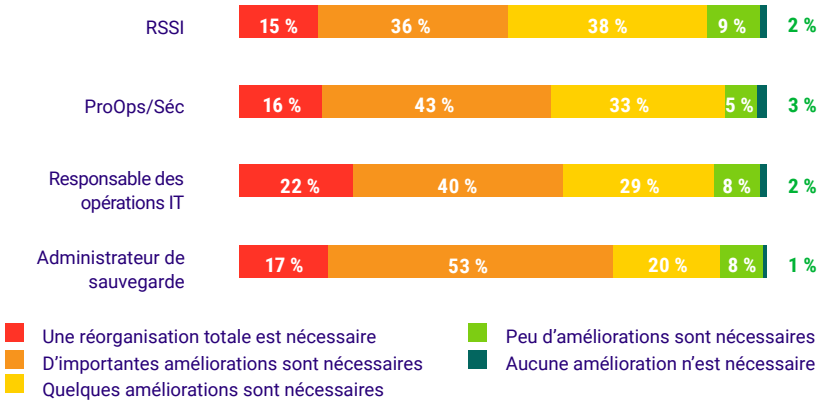


Figure 4.1

Selon vous, quelle est l'ampleur des améliorations nécessaires pour coordonner parfaitement les équipes chargées de la sauvegarde informatique et de la cybersécurité dans votre entreprise ?

Tandis qu'une majorité des sujets abordés dans ces enquêtes concernent les technologies utilisées ou les raisons/stratégies influençant les choix technologiques, les résultats révèlent aussi un manque net et constant de coordination entre les profils concernés. [17]

Il est important de noter que sur les quatre profils interrogés dans le cadre du rapport sur les tendances des ransomwares en 2023, plus le professionnel est « proche » de la fonction de correction de l'événement (administrateur de sauvegarde contre RSSI, par exemple), moins il est satisfait de la collaboration et de la coordination entre les équipes.

On constate des discordances du même ordre entre les administrateurs de sauvegarde et SaaS concernant la logique et les outils de protection Microsoft 365, ainsi qu'entre les administrateurs de sauvegarde et IaaS/PaaS concernant les stratégies et outils de protection des serveurs, partages de fichiers et bases de données dans le cloud.

Des questions à se poser !

Sur la base des retours de plus de 7 000 professionnels interrogés pendant huit mois, nous avons répertorié quelques questions utiles pour élaborer votre stratégie de cyber-résilience.

- Nos sauvegardes sont-elles à fois inaltérables et hors site ? Nos sauvegardes sont-elles gérées par un fournisseur expérimenté ou par nous-mêmes ?
- Pouvons-nous utiliser une infrastructure cloud comme site de reprise après incident ? Si la réponse est non, pourquoi ?
- Sauvegardons-nous toutes nos données hébergées dans le cloud, y compris les workloads IaaS, PaaS et SaaS ? Le cas échéant, utilisons-nous des outils distincts selon les clouds ou déployés de manière cohérente sur tous les clouds (et workloads locaux) ?
- Nos équipes sont-elles coordonnées en matière de sauvegarde locale, IaaS, PaaS et SaaS ?
- Nos équipes sont-elles coordonnées entre la prévention des risques cyber et la sauvegarde des données ?
- À quand remonte notre dernier test de restauration des données hébergées dans le cloud ?
- À quand remonte notre dernier test de restauration du datacenter à grande échelle ?
- À quand remonte la dernière évaluation et mise à jour de nos guides cyber et BC/DR ?

Pour toute question sur ces études ou leurs enjeux, contactez StrategicResearch@veeam.com.

Les rapports mentionnés peuvent être consultés intégralement ici :

- **Tendances de la protection du cloud en 2023**
  Enquête auprès de 1 700 administrateurs IaaS, PaaS et SaaS au sujet de leurs stratégies de protection des données.
- **Rapport sur les tendances de la protection des données en 2023**
  Enquête auprès de 4 200 décideurs IT responsables de la stratégie de protection des données de leur entreprise.
- **Rapport sur les tendances des ransomwares en 2023**
  Enquête auprès de 1 200 RSSI et professionnels de la sécurité/sauvegarde d'une entreprise victime d'une cyberattaque en 2022.

La perspective Veeam

Plateforme de sauvegarde et de gestion des données de Veeam

Aujourd'hui plus que jamais, les établissements doivent avoir la certitude que leurs données sont protégées et disponibles en permanence, que ce soit en local, en périphérie ou dans le cloud. Veeam propose une plateforme unique pour les environnements cloud, virtuels, physiques, SaaS et Kubernetes. Nos clients nous font confiance : ils savent que leurs applications et leurs données sont protégées contre les ransomwares, les sinistres et les acteurs malveillants, et qu'elles sont toujours disponibles grâce à la plateforme la plus simple, la plus flexible, la plus fiable et la plus puissante du marché.

Veeam leur permet d'accélérer leur transformation numérique, de se protéger contre la cybercriminalité et de favoriser la résilience de leur activité, tout en garantissant la protection et la disponibilité de leurs données. Réduisez vos coûts, simplifiez les processus et atteignez vos objectifs avec Veeam, le nº 1 de la sauvegarde et de la restauration.

Pour en savoir plus, rendez-vous sur **https://www.veeam.com/fr**.

Pour rencontrer un expert Veeam du cloud hybride, demandez une consultation **http://vee.am/hybridcloudinquiry**.

Adressez toute question sur les données et enseignements de ces études à StrategicResearch@veeam.com.

1 Rapport sur les tendances des ransomwares en 2023, Q29
2 Rapport sur les tendances des ransomwares en 2023, Q25
3 Rapport sur les tendances de la protection des données en 2023, Q45
4 Rapport sur les tendances de la protection des données en 2023, Q46
5 Rapport sur les tendances des ransomwares en 2023, Q21
6 Rapport sur les tendances des ransomwares en 2023, Q2
7 Rapport sur les tendances de la protection des données en 2023, Q13 et Q14
8 Rapport sur les tendances des ransomwares en 2023, Q9
9 Rapport sur les tendances des ransomwares en 2023, Q6
10 Rapport sur les tendances de la protection des données en 2023, Q6
11 Rapport sur les tendances de la protection du cloud en 2023, Q8
12 Rapport sur les tendances de la protection des données en 2023, Q17
13 Rapport sur les tendances de la protection des données en 2023, Q4
14 Rapport sur les tendances de la protection du cloud en 2023, Q35
15 Rapport sur les tendances des ransomwares en 2023, Q17
16 Rapport sur les tendances de la protection du cloud en 2023, Q4
17 Rapport sur les tendances des ransomwares 2023, Q1