Magic Quadrant pour les solutions logicielles de sauvegarde et de récupération pour entreprise

Publié le 7 août 2023 - ID G00776884 - Lecture : 43 minutes

Par les analystes : Michael Hoeck, Nik Simpson, Jerry Rozeman, Jason Donham

Les entreprises étendent leur utilisation des environnements hybrides et multicloud ainsi que des applications SaaS tout en faisant face à la menace adaptative des attaques par ransomware. Dans un tel contexte, les responsables I&O doivent évaluer en continu leurs capacités de sauvegarde et de récupération. Cette étude présente des analyses des fournisseurs de sauvegarde et de récupération.

Définition/description du marché

Gartner définit les solutions logicielles de sauvegarde et de récupération d'entreprise comme des solutions développées par des fournisseurs capturant une copie ponctuelle (sauvegarde) des charges de travail d'entreprise dans des environnements sur site, hybrides, multicloud et SaaS. Ces solutions écrivent les données sur une cible de stockage secondaire afin de récupérer ces données en cas de perte. Elles peuvent être proposées en tant qu'appliance logicielle, matérielle ou virtualisée, ou en tant que sauvegarde en tant que service (BaaS) basée sur SaaS.

La protection et la récupération des données des applications métier, quels que soient le type et l'emplacement de l'infrastructure sous-jacente, sont désormais plus critiques que jamais. Alors que les entreprises évoluent vers des environnements plus complexes qui incluent des quantités massives de données, les solutions logicielles de sauvegarde et de récupération d'entreprise sont censées protéger ces charges de travail, qu'elles résident dans des environnements sur site, hybrides, multicloud ou SaaS.

Les solutions logicielles de sauvegarde et de récupération d'entreprise sont essentielles pour permettre à une organisation de récupérer des données suite à des événements qui les rendent inaccessibles. Qu'il s'agisse d'un événement accidentel, malveillant ou environnemental, les organisations tirent parti de ces solutions pour récupérer et restaurer efficacement l'accès aux données affectées.

Les solutions doivent offrir des capacités efficaces pour simplifier la gestion de la protection des données dans les environnements d'entreprise complexes. Elles doivent également pouvoir garantir une récupération fiable en protégeant les données de sauvegarde contre un paysage de menaces en constante évolution, et accélérer et orchestrer les réponses relatives à la

récupération de données en cas de sinistres traditionnels et d'événements impliquant des attaques par ransomware.

Les capacités qu'une solution de sauvegarde et de récupération doit absolument avoir comprennent :

- la sauvegarde et la récupération des données situées dans l'infrastructure du centre de données sur site, ceci incluant les systèmes d'exploitation, les fichiers, les bases de données, les machines virtuelles et les applications ;
- la sauvegarde et la récupération des données situées dans l'infrastructure de cloud public, y compris le cloud multicloud et hybride, les architectures et les environnements comme infrastructure en tant que service (IaaS), plateforme en tant que service (PaaS) et SaaS ;
- la sauvegarde et la récupération des données situées dans l'infrastructure de cloud public, y compris le cloud multicloud et hybride, les architectures et les environnements comme infrastructure en tant que service (IaaS), plateforme en tant que service (PaaS) et SaaS ;
- l'attribution de plusieurs politiques de sauvegarde et de conservation conformes aux objectifs de récupération ponctuelle de l'organisation ;
- la création de rapports sur les succès et échecs des tâches de sauvegarde/récupération.

Les capacités normales d'une solution de sauvegarde et de récupération comprennent :

- la sauvegarde des données sur plusieurs cibles, y compris le cloud public, le fournisseur de sauvegarde et de récupération et le stockage d'objets ;
- l'intégration avec cible(s) de stockage de sauvegarde immuable ou stockage immuable propre au fournisseur de sauvegarde et de récupération ;
- l'orchestration de tests et de processus de reprise après sinistre et attaque par ransomware ;
- une console centralisée pour la gestion de l'infrastructure de la solution de sauvegarde distribuée.

Les capacités facultatives susceptibles d'être fournies par la solution comprennent :

- l'extension des cas d'utilisation des données de sauvegarde pour prendre en charge la découverte des données, la conformité, la gestion des données de copie, les tests/développement et la découverte électronique ;
- la protection des autres charges de travail, y compris les conteneurs, le stockage d'objets, les sites distants/Edge et les endpoints ;
- la détection des anomalies de données dues à des ransomwares et la détection des logiciels malveillants développées ou intégrées par le fournisseur ;

- des coffres de données immuables et/ou des environnements de récupération isolés ;
- une récupération bare-metal.

Magic Quadrant

Figure 1 : Magic Quadrant pour les solutions logicielles de sauvegarde et de récupération pour entreprise

Points forts et réserves concernant les fournisseurs

Acronis

Acronis est un Acteur de niche de ce Magic Quadrant. Le portefeuille de sauvegarde d'Acronis se compose de sa solution sur site Acronis Cyber Protect et hébergée dans le cloud offrant Acronis Cyber Protect Cloud. Tous deux offrent une sauvegarde intégrée, une sécurité et une gestion des

endpoints pour les serveurs physiques, les machines virtuelles (VM) sur site, les charges de travail SaaS, les charges de travail IaaS sur cloud public et les endpoints. La plupart de ses clients se situent dans le marché intermédiaire. Les produits sont distribués par une force de vente directe et plus de 20 000 prestataires de services dans 52 centres de données Acronis répartis dans toutes les principales zones géographiques. Au cours de la période d'évaluation, Acronis a ajouté plusieurs nouvelles fonctionnalités. Il s'agit notamment de la prise en charge de la fonction de verrouillage de la rétention Dell PowerProtect DD, de la récupération en un clic, d'une récupération initiée par l'utilisateur final à partir de la dernière sauvegarde connue, de la validation de sauvegarde assistée par machine learning (ML), de la récupération après sinistre et de la reprise après sinistre des machines virtuelles Microsoft Azure vers le cloud Acronis.

Points forts

- **Capacités intégrées de cyberprotection et de protection des données pour les endpoints, les serveurs d'applications et les déploiements IaaS sur cloud public** : Acronis propose une offre unique basée sur un agent qui combine la sécurité, la sauvegarde et la reprise après sinistre ainsi qu'une gestion informatique pour les endpoints, les postes de travail, les serveurs d'applications et les déploiements IaaS sur cloud public dans Azure et AWS.

- **Prise en charge étendue des hyperviseurs** : Acronis offre une prise en charge d'un large éventail d'hyperviseurs au-delà de VMware et Microsoft, comme Citrix XenServer, Virtuozzo, Red Hat, Oracle VM, Nutanix, Linux KVM et Scale Computing.

- **Couverture mondiale dans plusieurs langues** : Acronis offre une solution de protection des données différenciée et disponible dans le monde entier pour les sites distants/emplacements de serveurs Edge et les endpoints, localisée dans plus de 25 langues.

Réserves

- **Capacités cloud public et d'entreprise limitées** : Acronis manque de capacités entreprise essentielles, avec une prise en charge limitée des bases de données d'entreprise, des architectures de clusters, des systèmes d'exploitation, du stockage en réseau (NAS), de l'intégration du stockage d'entreprise, du regroupement de stockage, de la déduplication et de la prise en charge des applications de cloud public.

- **Évolutivité limitée** : l'architecture de stockage de sauvegarde directe configurée par l'agent d'Acronis est moins adaptée aux déploiements de grandes entreprises, car des fonctionnalités d'entreprise demeurent manquantes et l'évolutivité est limitée.

- **Accent commercial sur les fournisseurs de services gérés (MSP)** : Acronis se concentre principalement sur la vente par le biais de MSP pour fournir une solution gérée offrant la sauvegarde, la reprise après sinistre, la cybersécurité, la collaboration et la gestion des endpoints. Avec cette approche de mise sur le marché, les relations commerciales et l'expérience client, ceci incluant l'assistance, la sécurité et la performance, seront principalement de la responsabilité du MSP choisi.

Arcserve

Arcserve est un Challenger de ce Magic Quadrant. Le portefeuille de sauvegarde d'Arcserve comprend Arcserve UDP, Arcserve Backup, les appliances Arcserve UDP, Arcserve Cloud Direct, Arcserve UDP Cloud Hybrid Secured by Sophos, les appliances de stockage Arcserve OneXafe et Arcserve SaaS Backup. Les opérations d'Arcserve sont géographiquement diversifiées, et la majeure partie de ses clients se trouve dans le segment du marché intermédiaire. Au cours de la période d'évaluation, Arcserve a lancé UDP 9.0, qui comprenait des améliorations pour la prise en charge de base de données, une console de gestion multi-tenant hébergée dans le cloud et basée sur SaaS, et la possibilité d'écrire des sauvegardes directement sur un stockage d'objets conforme à S3. En plus d'améliorations d'UDP, Arcserve a également modifié les appliances de sauvegarde et de stockage afin d'améliorer leurs performances et de les rendre plus évolutives.

Points forts

- **Prise en charge étendue de la charge de travail :** L'association d'Arcserve Backup et d'Arcserve UDP permet à Arcserve de prendre en charge de nombreuses charges de travail d'entreprise dans les centres de données et le cloud public. Cette prise en charge élargie de la charge de travail, associée à une plateforme évolutive et à plusieurs options d'intégration de cibles de stockage, peut protéger plusieurs pétaoctets de données.

- **Stockage d'objets directement sur le cloud :** UDP permet aux clients de sauvegarder des données directement sur le stockage d'objets dans le cloud avec déduplication. Il est compatible avec AWS S3, Wasabi et Google Cloud Storage.

- **Amélioration des performances et de la capacité des appliances de stockage OneXafe :** Les améliorations de OneXafe permettent des récupérations plus rapides et une plus grande échelle à un encombrement réduit avec un stockage SSD (solid-state drive) disponible et une capacité de disque individuelle supérieure à 24 TB

Réserves

- **Capacités de détection et de récupération limitées :** associé à l'anti-logiciel malveillant Sophos, Arcserve UDP manque de capacités de détection des anomalies et de conseils pour les points de récupération recommandés.

- **Immuabilité de OneXafe limitée :** la conception immuable des appliances de stockage OneXafe ne dispose pas de verrouillage du stockage d'objets ni de contrôles d'authentification-multipersonne, ce qui limite ses capacités optimales de protection contre les pertes de données dues à des attaques par ransomware et à des menaces internes.

- **Manque de sauvegarde de conteneur :** Arcserve ne fournit pas de capacités de sauvegarde pour les charges de travail de conteneur.

Cohesity

Cohesity est un Leader de ce Magic Quadrant. Son portefeuille de produits de sauvegarde comprend DataProtect et une offre BaaS appelée DataProtect fournie en tant que service. Les opérations de Cohesity sont réparties en Amérique du Nord, en Europe occidentale et en Asie/Pacifique. Ses clients se situent généralement dans les segments supérieurs du marché

intermédiaire et des entreprises. Au cours de la période d'évaluation, Cohesity a introduit un stockage de coffre-fort cloud géré par le fournisseur FortKnox, qui peut être combiné avec des capacités de détection des menaces et de classification des données via une nouvelle solution appelée DataHawk. Cohesity a ajouté des intégrations de base de données DataProtect pour étendre la couverture SAP et prendre en charge PostgreSQL et Couchbase. De plus, l'entreprise a annoncé un partenariat OEM avec IBM pour inclure sa protection des données à la nouvelle solution Storage Defender d'IBM.

Points forts

- **Une gestion unifiée et simplifiée :** Cohesity Helios, un plan de contrôle SaaS, offre une expérience administrative centralisée, commune et intuitive pour tous les produits de son offre de sauvegarde.
- **BaaS et stockage multicloud :** Cohesity DataProtect fourni en tant que service et les produits FortKnox permettent aux clients de choisir parmi plusieurs emplacements de stockage de plans de données cloud, y compris AWS et Azure.
- **Une stratégie d'alliance de sécurité :** Cohesity a engagé de manière proactive plusieurs fournisseurs dans des disciplines variées sur le marché de la sécurité. L'objectif de sa Data Security Alliance est de favoriser des solutions collaboratives et de développer des produits intégrés pour répondre plus largement aux préoccupations des clients en matière de sécurité et de résilience des données.

Réserves

- **De nouveaux investissements introduisent la dépendance à la technologie tierce :** la solution DataHawk de Cohesity comprend des dépendances à l'égard de deux nouveaux partenariats OEM pour renforcer ses investissements dans des offres complémentaires récentes.
- **Capacités BaaS limitées par rapport à celles gérées par le client :** les produits Cohesity et les fonctionnalités connexes de FortKnox et DataHawk ne sont pas encore disponibles pour les clients qui protègent leurs données grâce à DataProtect, l'offre BaaS fournie en tant que service de Cohesity.
- **Couverture géographique réduite :** Cohesity est à la traîne par rapport aux autres fournisseurs leaders en termes de présence sur le marché et d'exécution en Amérique du Sud.

Commvault

Commvault est un Leader de ce Magic Quadrant. Son portefeuille comprend Commvault Backup & Recovery, Commvault Disaster Recovery, Commvault HyperScale X, Metallic SaaS portfolio et Metallic ThreatWise. Les opérations de Commvault sont géographiquement diversifiées, et ses clients ont tendance à être de grandes entreprises. Au cours de la période d'évaluation, Commvault a introduit la prise en charge de MongoDB Atlas, Hyper-V Live Recovery, Couchbase et Amazon VPC Protection, ainsi qu'une fonctionnalité analysant le contenu de sauvegarde pour détecter les logiciels malveillants pendant la récupération. Commvault a amélioré son offre Metallic en ajoutant la prise en charge des bases de données Azure, y compris SQL Server,

Cosmos DB, MariaDB, MySQL et PostgreSQL, ainsi que la prise en charge des restaurations en libre-service pour Exchange Online et OneDrive.

Points forts

- **Portée de la couverture BaaS** : la couverture complète de Commvault Metallic en matière d'applications SaaS, de multicloud, sur site et de endpoints est complétée par l'ajout de la protection Oracle Cloud Infrastructure (OCI), votre propre stockage d'objets OCI, de nouvelles offres Metallic File and Object Archive et Metallic ThreatWise.

- **Une interopérabilité logicielle complète** : le logiciel Commvault Backup & Recovery offre une large couverture et des capacités pour les environnements sur site, hybrides et multicloud. La prise en charge du cloud public inclut désormais une prise en charge étendue d'Azure, AWS, GCP et OCI.

- **Des fonctionnalités d'entreprise à des tarifs compétitifs** : Commvault a fixé le prix de ses licences par machine virtuelle pour Commvault Backup & Recovery afin d'entrer dans de nouveaux segments de marché qui auraient pu être indisponibles auparavant.

Réserves

- **Par rapport à la cadence de mise à jour du cloud, les innovations sur site sont à la traîne** : la stratégie produit de Commvault met à jour Metallic BaaS avant que des fonctionnalités équivalentes soient disponibles pour les produits Commvault Complete Data Protection et HyperScale X. Il en résulte que de nouvelles fonctionnalités sont initialement disponibles pour le sous-ensemble basé sur le cloud de la clientèle de Commvault.

- **Une expérience client Commvault Metallic variable** : certains clients de Gartner ont évoqué les défis associés aux performances incohérentes et aux difficultés de configuration initiales de Metallic.

- **Des capacités de gestion incohérentes** : les évaluations de Gartner Peer Insights indiquent que la commande et le contrôle unifiés entre l'interface utilisateur HTML5 du centre de commande Commvault ne disposent pas de certaines fonctionnalités de la console d'application locale.

Dell Technologies

Dell Technologies est un Leader de ce Magic Quadrant. Son portefeuille de logiciels de sauvegarde et de récupération comprend PowerProtect Data Manager, PowerProtect Cyber Recovery, CyberSense, Dell NetWorker, Dell Avamar, Dell APEX Backup Services, PowerProtect série DP et les appliances PowerProtect série DD. Les opérations de Dell sont géographiquement diversifiées, et ses clients ont tendance à être de grandes entreprises, avec une présence sur le marché intermédiaire. Au cours des 12 derniers mois, Dell Technologies a amélioré PowerProtect Data Manager pour inclure la sauvegarde et la récupération de Microsoft Distributed File System, la récupération au niveau des fichiers pour la protection NAS dynamique et la prise en charge de PowerProtect Cloud Snapshot Manager pour Google Cloud. Les nouvelles offres comprennent PowerProtect Data Manager Appliance (DM5500), PowerProtect Cyber pour Azure et Google, et CyberSense pour AWS.

Points forts

- **PowerProtect Cyber Recovery pour cloud et sur site** : la solution de récupération de coffre-fort de données et après attaque par ransomware de Dell, appelée PowerProtect Cyber Recovery, inclut désormais des options de déploiement pour les environnements cloud AWS, Azure et Google, et sur site.

- **Évolutivité de l'appliance PowerProtect DD** : l'introduction de Smart Scale par Dell permet aux clients de PowerProtect Data Manager de combiner la capacité de plusieurs appliances DD PowerProtect, ce qui permet un équilibrage et une migration simplifiés des données de sauvegarde entre elles.

- **Prise en charge et disponibilité multicloud de PowerProtect Data Manager** : PowerProtect Data Manager fournit une prise en charge cohérente et complète des charges de travail dans AWS, Azure et GCP. Il est également facilement disponible sur les marchés respectifs et inclut une licence pour APEX Protection Storage.

Réserves

- **Aucun plan de contrôle basé sur SaaS** : Dell ne dispose pas d'un plan de contrôle SaaS complet, ni d'une interface administrative commune pour tous les composants de sa solution, alors que les deux sont généralement présents dans les solutions des principaux fournisseurs.

- **Des options de stockage de sauvegarde limitées** : les appliances DD PowerProtect restent exigées pour l'utilisation de la plupart des solutions de protection des données Dell, limitant l'utilisation de cibles de sauvegarde alternatives.

- **L'analyse avancée des données de ransomware nécessite un environnement dédié** : la détection avancée des anomalies et des logiciels malveillants nécessite une appliance DD PowerProtect séparée et dédiée, ainsi qu'une infrastructure de calcul supplémentaire.

Druva

Druva est un Visionnaire de ce Magic Quadrant. La plateforme Druva Data Resiliency Cloud est une offre BaaS qui exploite l'infrastructure AWS pour exécuter, stocker et gérer les sauvegardes. La plateforme se compose de plusieurs produits qui fournissent une sauvegarde et une reprise après sinistre sur site et dans le cloud, une sauvegarde et une reprise après sinistre natives dans le cloud AWS et Kubernetes, ainsi qu'une sauvegarde des applications SaaS et des endpoints. Les opérations de Druva sont géographiquement diversifiées, avec la plupart de ses clients en Amérique du Nord. Ses clients appartiennent généralement aux segments des moyennes et grandes entreprises. Au cours de la période d'évaluation, Druva a ajouté Salesforce Data Archiver, Data Lock, Unusual Data Activity et de nouvelles intégrations comme Windows Server 2022 Hyper-V virtual machine hosts, SAP HANA, VMware on Azure, VMs on Azure Stack et AWS S3. Druva a également amélioré la prise en charge de Nutanix AHV et accéléré la sauvegarde incrémentielle pour NAS avec Advanced Smart Scan.

Points forts

- **Portée de la garantie** : la garantie de résilience des données de Druva offre une gamme complète d'objectifs de niveau de service, y compris le taux de réussite des sauvegardes, la disponibilité, l'immuabilité, la durabilité et la confidentialité.

- **Architecture de solution BaaS cloud native** : en s'appuyant sur sa solution BaaS mature, Druva a réalisé un investissement significatif dans une refonte sans interruption de sa plateforme d'architecture de sauvegarde pour établir un nouveau cadre favorable à l'évolutivité, à l'agilité et aux capacités multicloud futures.

- **Expérience client du centre de données au cloud** : de nombreux clients font part d'une expérience positive dans l'utilisation de la BaaS de Druva pour protéger les données d'application SaaS, les environnements sur site et les machines virtuelles cloud.

Réserves

- **Des capacités de protection de la charge de travail cloud natives limitées** : par rapport aux principaux fournisseurs, Druva a mis du temps à étendre ses offres de protection cloud natives. Il manque une intégration sans agent avec Azure VM, Google Compute Engine (GCE) et OCI. Les intégrations de charge de travail avec Azure SQL, Azure Blob Storage, MongoDB et Cassandra ne sont pas prises en charge.

- **Capacités multicloud restreintes** : la solution BaaS de Druva reste uniquement basée sur l'architecture cloud AWS pour ses plans de contrôle et de données. Elle est à la traîne par rapport aux principaux fournisseurs qui offrent au client le choix des emplacements de plans de données multicloud pour leurs offres de stockage BaaS et fournisseur.

- **Il ne prend pas en charge MS Dynamics, Azure AD, ServiceNow, Azure DevOps et Intégration moins complète de la sauvegarde des applications SaaS** : l'expansion de Druva en matière de protection des nouvelles applications SaaS est limitée. GitHub.

HYCU

HYCU est un Visionnaire de ce Magic Quadrant. HYCU Protégé est une plateforme BaaS hybride et multicloud qui couvre Azure, AWS et Google pour prendre en charge les charges de travail IaaS, DBaaS, PaaS, SaaS et sur site. Les opérations d'HYCU sont géographiquement diversifiées, la majorité de ses clients se situant en Amérique du Nord. Ses clients se situent généralement dans les segments supérieurs du marché intermédiaire. Au cours de la période d'évaluation, HYCU a introduit plusieurs nouvelles fonctionnalités telles qu'un niveau gratuit pour AWS, une prise en charge supplémentaire d'Azure Government, une sauvegarde de partage de fichiers sans impact et des charges de travail Edge et ROBO. En outre, HYCU a introduit R-Cloud, une plateforme de développement Low Code permettant aux fournisseurs de développer une sauvegarde SaaS sur la plateforme HYCU, ainsi que R-Graph, un outil de cartographie de l'observabilité et des dépendances pour les charges de travail SaaS.

Points forts

- **Facilité d'utilisation** : les demandes des clients de Gartner indiquent un niveau élevé de satisfaction pour la facilité d'utilisation, la stabilité du produit et la gestion de la sauvegarde et

de la reprise après sinistre pour la solution de gestion hybride HYCU Protégé.
- **Prise en charge multicloud et hybride** : HYCU Protégé simplifie la protection des environnements multicloud et hybrides en prenant en charge les charges de travail Azure, AWS, Google et de centre de données grâce à une solution SaaS unifiée unique.

- **Sauvegarde SaaS** :R-Cloud peut accélérer la prise en charge de la sauvegarde SaaS au-delà des applications SaaS les plus populaires, comme Microsoft 365 et Salesforce.

Réserves
- **Limitations sur site** : l'offre sur site d'HYCU est en retard par rapport aux principaux fournisseurs en termes de fonctionnalités comme la déduplication globale des données, la protection continue des données (CDP), la prise en charge des charges de travail de conteneur et des clusters d'entreprise comme Oracle RAC, et la prise en charge des charges de travail non x86 comme Power/AIX.

- **Capacités limitées de détection des ransomwares** : HYCU manque de capacités de détection avancée des ransomwares basée sur l'analyse des données de sauvegarde, comme la détection d'entropie et de chiffrement, et de guidage vers les points de récupération disponibles dans les offres concurrentes.

- **Client responsable du stockage et de la sécurité sur site** : HYCU n'a aucun contrôle direct sur le stockage sur site et la sécurité du stockage, ce qui rend les clients responsables de la mise en place d'une solution sécurisée pour protéger les sauvegardes contre les cyberattaques.

IBM

IBM est un Visionnaire de ce Magic Quadrant. Son portefeuille de sauvegarde principal comprend IBM Storage Protect, IBM Storage Protect Plus, IBM Storage Protect Snapshot, IBM Storage Copy Data Management et IBM Storage Protect for Cloud. Les opérations d'IBM sont géographiquement diversifiées, et ses clients ont tendance à être de grandes entreprises. Au cours de l'année écoulée, le fournisseur a introduit quatre mises à jour pour Storage Protect et Storage Protect Plus. Les ajouts de Storage Protect incluent le stockage immuable sur IBM Cloud Object Storage, le verrouillage d'objet sur Amazon S3 et les mises à jour du centre d'opérations. Les ajouts de Storage Protect Plus incluent la prise en charge des clusters Red Hat OpenShift pour IBM Z, SAP HANA et la sauvegarde incrémentielle pour les conteneurs. Storage Protect for Cloud a introduit la prise en charge d'Azure VM, BLOB, AD and File, Salesforce et Microsoft Dynamics 365.

Points forts
- **Stratégie produit** : IBM a annoncé un changement stratégique dans ses offres de sauvegarde et de récupération en les intégrant à sa gamme de produits de stockage primaire et à plusieurs produits OEM complémentaires. Storage Defender est en mesure de fournir une solution de cyberprotection intégrée et unifiée sous un plan de contrôle commun. IBM s'est associé à Cohesity pour remplacer ses capacités actuelles de protection des machines virtuelles et fournir le nouveau plan de contrôle basé sur SaaS.

- **Sauvegarde de conteneur OpenShift :** IBM a continué à réaliser des investissements importants dans IBM Storage Protect Plus pour la sauvegarde et la récupération via Red Hat OpenShift Kubernetes et IBM Cloud Paks. Les ajouts récents incluent la protection des environnements Red Hat OpenShift connectés aux clusters, des ressources étendues aux clusters et à l'espace de noms, ainsi que des intégrations CSI mises à jour avec Ceph, le stockage en bloc IBM et le NAS Hitachi.

- **Protection Microsoft 365 :** IBM Storage Protect for Cloud offre aux utilisateurs finaux une restauration en libre-service pour Microsoft Exchange Online, SharePoint Online, Teams, OneDrive et Groups.

Réserves

- **Changement de portefeuille en cours :** la stratégie et l'exécution d'IBM sur le changement de portefeuille annoncé sont en cours. Ce nouveau portefeuille aura un impact sur les clients existants et potentiels à mesure que de nouveaux produits de remplacement seront lancés. Les clients d'IBM auront besoin de plusieurs produits, basés sur un plus grand nombre de technologies ISV et OEM, pour répondre à leurs exigences en matière de protection des données multicloud et hybrides.

- **Exécution limitée :** IBM a souvent changé sa vision et sa stratégie produit pour l'intégration et le positionnement des anciens produits Spectrum Protect et Spectrum Protect Plus, et n'a montré qu'un succès limité dans l'exécution de ces changements. Cela inclut les efforts antérieurs visant à positionner Spectrum Protect Plus comme son offre leader sur le marché.

- **Capacités limitées de récupération multi-plateforme :** IBM Storage Protect Plus nécessite des solutions de reprise après sinistre intégrées au client ou à l'API ISV, ou l'utilisation de solutions partenaires ISV pour prendre en charge la reprise multi-plateforme.

Microsoft

Microsoft est un Acteur de niche et un nouvel entrant dans ce Magic Quadrant. Son portefeuille de sauvegarde et de récupération comprend Azure Backup, Azure Site Recovery (ASR), Microsoft Azure Backup Server (MABS), System Center Data Protection (DPM) et Microsoft Azure Recovery Services (MARS). Les opérations de Microsoft sont géographiquement diversifiées et ses clients sont généralement de toutes tailles. Au cours des 12 derniers mois, Microsoft a apporté plusieurs améliorations à Azure Backup, comme Azure Backup Instant Restore, Cross Zonal Restore of Azure VMs, Azure Vault-Archive, la hiérarchisation intelligente, l'analyse des coûts de sauvegarde, les coffres immuables, l'authentification multi-utilisateurs et l'amélioration du chiffrement.

Points forts

- **Offre optimisée pour les clients dédiés de Microsoft :** Azure Backup et Azure Site Recovery sont des offres adaptées à la sauvegarde et à la reprise après sinistre qui protègent les charges de travail d'un large éventail de clients (des petites aux grandes entreprises) utilisant principalement des machines virtuelles Microsoft Windows et Azure sur site.

- **Une feuille de route complète :** Microsoft offre une feuille de route très complète, avec une intégration approfondie des fonctionnalités existantes et à venir pour améliorer son portefeuille de sécurité de sauvegarde avec plusieurs fonctionnalités en mode aperçu public ou privé.

- **Coût total de possession (CTP) réduit :** Azure Backup et Azure Site Recovery offrent un faible coût total de possession par rapport aux offres tierces concurrentes.

Réserves

- **Couverture minimale de la charge de travail :** la matrice de support de sauvegarde Azure est limitée à la protection des serveurs Microsoft Windows Server ou des machines virtuelles Microsoft Windows, des machines virtuelles Azure, de SQL Server dans Azure VM, de SAP HANA dans Azure VM, des fichiers Azure, d'Azure Postgres, d'Azure Blobs et d'Azure Disks. Les autres services PaaS et SaaS de Microsoft comme Azure SQL Server, Azure AD, Azure DevOps, Dynamics 365 et Microsoft 365 ne sont pas couverts.

- **Pas de prise en charge multicloud :** la sauvegarde Azure ne prend pas en charge la protection d'AWS, de Google ou d'autres services cloud ou SaaS, car elle est dédiée à Azure et aux charges de travail sur site.

- **Offre de produits qui se chevauchent :** les options de sauvegarde et de récupération Microsoft sont un mélange complexe de produits multiples, interconnectés et redondants.

OpenText

OpenText est un Acteur de niche de ce Magic Quadrant. L'entreprise a finalisé son acquisition de Micro Focus en janvier 2023. Son portefeuille de produits de sauvegarde d'entreprise se compose principalement de deux produits : Protection des données pour les charges de travail sur site et protection des données pour les charges de travail cloud couvrant les charges de travail IaaS et SaaS cloud. Les opérations du fournisseur sont géographiquement diversifiées, et ses clients se trouvent dans le segment du marché intermédiaire. Au cours de l'année passée, OpenText a amélioré sa protection des données en développant la prise en charge de SAP HANA, le contrôle d'accès basé sur les rôles (RBAC), MongoDB et la déduplication. Data Protector for Cloud Workloads a ajouté la prise en charge des machines virtuelles pour Azure Cloud, Azure Stack HCI, Google Cloud et Virtuozzo, ainsi que des intégrations améliorées d'exportation et d'API pour Microsoft 365.

Points forts

- **Tarification basée sur la capacité :** OpenText a amélioré son modèle de licence en simplifiant un grand nombre de SKU en un seul numéro de pièce basé sur la capacité. Cette approche offre aux clients une option de dépenses d'exploitation facilement compréhensible pour entrer dans un modèle de tarification basé sur la capacité et le paiement à l'utilisation.

- **Prise en charge traditionnelle des centres de données d'entreprise :** Data Protector dispose de vastes capacités de sauvegarde de centres de données. Il prend en charge un grand nombre de charges de travail à faible coût total de possession par rapport aux autres fournisseurs.

- **Prise en charge étendue des cibles de stockage :** Data Protector prend en charge une large gamme d'appliances de sauvegarde spécialement conçues, de protocoles de stockage multiples et de bibliothèques de bandes.

Réserves

- **Manque de détection des anomalies et des logiciels malveillants :** Data Protector accuse un net retard par rapport aux autres fournisseurs en matière de fonctionnalités de détection des anomalies et des logiciels malveillants. Ces capacités font partie de l'écosystème OpenText, mais n'ont pas encore été intégrées à Data Protector.

- **Intégration des produits de base :** la couverture d'une gamme complète de charges de travail de datacenter et de cloud nécessite deux produits distincts : Protecteur de données et protecteur de données pour les charges de travail cloud, qui n'ont pas d'intégration significative.

- **Positionnement peu clair du produit :** à l'heure actuelle, il n'est pas clair si la technologie du produit sera entièrement intégrée dans le portefeuille OpenText plus large ou si elle continuera en tant que produit autonome.

Rubrik

Rubrik est un Leader de ce Magic Quadrant. Son portefeuille de produits de sauvegarde comprend Rubrik Security Cloud, qui inclut plusieurs offres de sauvegarde, de sécurité des données et de récupération avancée. Les activités de Rubrik sont géographiquement diversifiées et ses clients sont principalement de grandes entreprises. Au cours de la période d'évaluation, Rubrik a introduit plusieurs fonctionnalités nouvelles ou améliorées. Il s'agit notamment d'un nouveau modèle d'apprentissage automatique pour la détection des ransomwares, la prise en charge de la détection des ransomwares dans les hyperviseurs Nutanix et Microsoft, une meilleure récupération pour les environnements VMware, un centre de commande de sécurité des données qui aide les organisations à évaluer leur posture de sécurité globale, et des fonctionnalités de confinement des menaces pour isoler les malwares dans les sauvegardes.

Points forts

- **Innovation dans la stratégie produit, la tarification, la stratégie de marque et le regroupement :** Rubrik propose une approche innovante pour étendre ses offres axées sur la sécurité à la sauvegarde et à la restauration via de nouvelles options de tarification, avec des niveaux d'utilisateurs compétitifs et basés sur la capacité pour Microsoft 365, et en simplifiant la stratégie de marque et le regroupement de packages de produits.

- **Fonctionnalités de protection et de récupération après attaque par ransomware :** Rubrik propose une offre de produits complète et sécurisée qui protège le système de sauvegarde et les données contre les cyberattaques, y compris des capacités de détection des anomalies et des logiciels malveillants dans les données de sauvegarde, et fournit des fonctionnalités de récupération efficaces.

- **Adoption par entreprise :** les capacités d'évolutivité et le support client différencié de Rubrik continuent d'attirer les grandes entreprises, remplaçant ainsi une variété de solutions concurrentes.

Réserves

- **Équilibre entre sécurité et sauvegarde :** certains clients se sont inquiétés de la capacité de Rubrik à équilibrer ses initiatives d'offre de sécurité des données tout en restant concentrés sur les exigences des marchés émergents en matière de sauvegarde.

- **Couverture limitée des applications SaaS :** Rubrik offre une prise en charge limitée des applications SaaS au-delà de Microsoft 365. La couverture n'est pas encore disponible pour les applications comme Salesforce, Google Workspace, Microsoft Dynamics 365, Azure AD, ServiceNow, Azure DevOps et GitHub.

- **Offres de stockage cloud géré par le fournisseur limitées :** Rubrik propose uniquement le stockage Azure pour ses solutions BaaS et de coffre-fort géré par le fournisseur.

Unitrends

Unitrends, une entreprise Kaseya, est un Acteur de niche de ce Magic Quadrant. Son portefeuille de sauvegarde comprend Unitrends Backup Software, Recovery Series Backup Appliance et la sauvegarde d'applications Spanning Backup for SaaS. Les opérations du fournisseur sont géographiquement diversifiées, et ses clients se trouvent dans le segment du marché intermédiaire. Au cours des 12 derniers mois, Unitrends a lancé une offre BaaS pour la sauvegarde et la reprise après sinistre de Microsoft Azure VM. Unitrends a également automatisé la gestion des licences pour la sauvegarde Microsoft 365 via Azure AD Security Groups, et amélioré la sécurité d'Unitrends avec une authentification à deux facteurs via UniView. De plus, Unitrends continue d'étendre l'intégration d'UniView à d'autres produits de gestion de la sécurité et de l'infrastructure Kaseya.

Points forts

- **Administration unifiée :** Unitrends UniView offre un accès administratif unique à tous les composants de la solution, ceci incluant gestion des appliances, sauvegarde des endpoints et les applications SaaS.

- **Portefeuille complet :** Unitrends continue d'étendre ses offres de logiciels et d'appliances avec l'ajout de services intégrés de reprise après sinistre dans le cloud.

- **Intégration de Kaseya :** Unitrends continue de concentrer son intégration dans le portefeuille Kaseya IT Complete. Cela simplifiera l'accès aux ressources techniques, de facturation et d'assistance, et fournira plus de fonctionnalités à ses clients.

Réserves

- **Adéquation entreprise limitée :** avec leur accent mis sur les marchés des petites et moyennes entreprises, les initiatives de croissance d'Unitrend et son évolutivité limitée des appliances contribuent à une adéquation limitée pour les grandes entreprises.

- **Capacités multicloud limitées** : Unitrends Backup pour Microsoft Azure ne prend en charge que les machines virtuelles Azure et ne prend pas en charge d'autres charges de travail dans Azure telles qu'Azure SQL et Azure Blob. l'expansion pour la prise en charge d'autres fournisseurs de cloud, tels qu'AWS et GCP, est en cours.

- **Stratégie BaaS limitée** : Unitrends est à la traîne par rapport aux autres acteurs majeurs, dont les solutions BaaS gérées par les fournisseurs prennent en charge plusieurs charges de travail cloud et sur site, ainsi que d'autres applications SaaS, telles qu'Azure AD, ServiceNow et Microsoft Dynamics 365.

Veeam

Veeam est un Leader de ce Magic Quadrant. Son portefeuille de sauvegarde se compose de Veeam Data Platform, qui est composé de Veeam Backup & Replication, Veeam ONE et Veeam Recovery Orchestrator.

Les opérations de Veeam sont géographiquement diversifiées, et ses clients se trouvent généralement dans les segments du marché intermédiaire et des entreprises petites et moyennes. Au cours des 12 derniers mois, Veeam a produit 24 mises à jour de produits, dont Veeam v12, qui contient plusieurs nouvelles fonctionnalités comme le stockage direct sur objet, l'immuabilité pour Azure, l'amélioration de la protection NAS, ainsi qu'une intégration plus approfondie avec Kasten. Veeam a également introduit de nouveaux forfaits de tarification contenant de nouvelles combinaisons de ses produits Data Platform.

Points forts

- **Une clientèle fidèle et satisfaite** : la croissance et la fidélisation des clients de Veeam, ainsi que le niveau de participation de ses clients dans les communautés de groupes d'utilisateurs et les forums comme Veeam Community, sont révélateurs d'une clientèle fidèle et satisfaite.

- **Prise en charge hybride et multicloud** : la plateforme de données Veeam est disponible pour les trois principaux fournisseurs de cloud public, où elle offre une expérience de récupération hybride, multicloud et intercloud cohérente pour les charges de travail les plus couramment utilisées.

- **Large réseau de partenaires et MSP** : les offres Veeam sont disponibles via un réseau mondial étendu de partenaires autorisés. incluant les partenaires revendeurs, alliance, mise en œuvre et MSP.

Réserves

- **Réponse lente aux tendances clés du marché** : Veeam a été lent à réagir aux tendances clés du marché ainsi qu'aux attentes des clients en offrant des services hébergés par les fournisseurs, comme BaaS, plan de contrôle basé sur SaaS et coffres-forts de stockage, ainsi que des capacités natives de détection des anomalies dues à des ransomware basées sur l'analyse des données.

- **Complexité globale :** les demandes de certains clients de Gartner indiquent que Veeam peut s'avérer plus complexe à gérer à mesure que la taille de l'environnement de sauvegarde augmente. Cela comprend le déploiement d'agents Veeam distincts par environnement protégé, la gestion de plusieurs proxys de sauvegarde et de stockage ainsi que la sélection et la gestion appropriées de l'infrastructure de calcul et de stockage pour s'aligner sur les exigences de performance et de stockage.

- **Sécurisé par l'exigence de mise en œuvre :** la mise en œuvre d'une plateforme de données Veeam sécurisée exige que les clients conçoivent, configurent et gèrent le déploiement de manière réfléchie pour atténuer les cybermenaces, en intégrant immuabilité et détection des ransomwares fournies par des solutions tierces.

Veritas

Veritas est un Leader de ce Magic Quadrant. Son portefeuille de produits de sauvegarde comprend NetBackup, NetBackup Appliances et Backup Exec, ainsi que ses offres cloud Veritas Alta, qui comprennent Alta View, Alta BaaS, Alta Data Protection, Alta Recovery Vault et Alta SaaS Protection. Les opérations de Veritas sont géographiquement diversifiées. Ses clients sont généralement de grandes entreprises, et l'entreprise est présente sur le marché intermédiaire. Au cours des 12 derniers mois, la société a introduit ses offres cloud Alta, y compris son plan de contrôle SaaS basé sur le cloud, BaaS, et a étendu la prise en charge des applications SaaS pour inclure la sauvegarde Salesforce et Google Workspace. NetBackup a ajouté la prise en charge de 13 nouvelles charges de travail PaaS de base de données, la récupération isolée sur les appliances Flex Scale, l'analyse des logiciels malveillants du NAS et l'immuabilité GCP.

Points forts

- **Options exhaustives de sauvegarde et de gestion :** les offres cloud Veritas Alta, combinées aux capacités du logiciel NetBackup et de ses appliances matérielles évolutives et évolutives, offrent aux entreprises clientes un portefeuille complet de capacités de sauvegarde et de récupération, ainsi que de multiples options de déploiement et de gestion.

- **Architecture cloud native :** les services NetBackup et Alta s'exécutent dans des clusters Kubernetes qui s'exécutent nativement dans Azure, AWS et GCP. Dans cette conception, les services de plan de données fonctionnent indépendamment du plan de gestion en vue de fournir une architecture multicloud élastique et intrinsèquement flexible.

- **Large couverture géographique :** Veritas et ses partenaires peuvent vendre, déployer et prendre en charge les solutions Veritas dans toutes les zones géographiques majeures. Cela permet aux clients ayant des responsabilités dans le monde entier de trouver plus facilement une solution de sauvegarde qui répond à leurs exigences techniques et commerciales.

Réserves

- **Certains produits cloud sont nouveaux sur le marché :** les nouvelles offres de gestion basées sur Alta BaaS et Alta View SaaS de Veritas sont nouvelles sur le marché. Il n'y a que peu de données disponibles concernant l'adoption du marché ou la satisfaction des clients,

nécessitant une preuve de concept (POC) complète pour déterminer les niveaux d'expérience client en matière d'intégration et de performance.
- **Stratégie de produits et services centrée sur l'entreprise** : Veritas se concentre principalement sur les grandes entreprises clientes dans sa stratégie de produits et services Alta et NetBackup, ce qui la rend potentiellement moins adaptée aux clients de taille moyenne, commerciaux et PME.

- **Prise en charge moins complète des applications SaaS** : Veritas est à la traîne par rapport aux autres fournisseurs pour prendre en charge d'autres applications SaaS comme Microsoft Azure AD, Azure DevOps, Microsoft Dynamics 365 et GitHub avec Alta BaaS.

Fournisseurs ajoutés et supprimés

Nous évaluons et modifions nos critères d'inclusion aux Magic Quadrants en fonction de l'évolution du marché. En raison de ces modifications, la combinaison de fournisseurs présents dans un Magic Quadrant peut changer au fil du temps. Si un fournisseur apparaît dans un Magic Quadrant une année, mais pas l'année suivante, cela n'indique pas forcément que nous avons changé d'opinion à son égard. La modification peut tout simplement être le résultat d'une évolution du marché, et donc des critères d'évaluation, ou encore d'un changement stratégique de ce fournisseur.

Ajoutés

Microsoft : ce fournisseur a satisfait aux critères d'inclusion de cette année.

OpenText : ce fournisseur a été inclus dans le Magic Quadrant de cette année après avoir finalisé l'acquisition de Micro Focus en janvier 2023.

Abandonnés

Zerto, une entreprise HPE : ce fournisseur n'a pas satisfait aux critères d'inclusion de cette année.

Critères d'inclusion et d'exclusion

Les critères suivants représentent les attributs spécifiques que les analystes estiment nécessaire pour être inclus dans cette recherche :

- Le fournisseur doit répondre au minimum à l'un des critères de chiffre d'affaires suivants. Le chiffre d'affaires doit provenir exclusivement de son portefeuille de produits de sauvegarde et de récupération. Ces revenus ne doivent pas inclure les revenus générés par les services de mise en œuvre, hébergeur BaaS ou offres des fournisseurs en services gérés.

  - Le fournisseur doit avoir généré des revenus de licence (perpétuels et/ou d'abonnement) et de maintenance (principes comptables généralement acceptés [PCGR]) supérieurs à 50 millions USD au cours des quatre derniers trimestres se terminant le 28 février 2023 (ou)

  - Le fournisseur doit avoir généré des licences (perpétuelles et/ou par abonnement) et des revenus de maintenance (PCGR) supérieurs à 25 millions USD, combinés à un taux de

croissance de 20 % en glissement annuel, au cours des quatre derniers trimestres se terminant le 28 février 2023.

- La/Les solution(s) de sauvegarde et de récupération qualifiante(es) du fournisseur doit(vent) être vendue(s) et commercialisée(s) essentiellement auprès des organisations du marché intermédiaire supérieur et grandes entreprises. Gartner définit le marché intermédiaire supérieur comme étant une organisation de 500 à 999 employés, et la grande entreprise comme une organisation de 1 000 employés ou plus.

- La solution de sauvegarde et de récupération éligible du fournisseur doit se concentrer sur la protection des clients entreprises opérant dans des environnements hybrides/multicloud, qui incluent des environnements de centre de données (centre de données traditionnel ou site de colocation) et des charges de travail IaaS et PaaS basées sur le cloud. La protection des sites distants est considérée comme une extension de ces capacités de base.

- Les nouveaux produits ou les mises à jour de produits existants ayant été lancés au cours des 12 derniers mois doivent être généralement disponibles au plus tard le 31 mars 2023 pour être pris en compte dans l'évaluation. Tous les composants doivent être publiquement disponibles, expédiés et inclus dans la liste de prix publiée par le fournisseur à cette date. L'expédition des produits après cette date ne peut avoir qu'une influence sur l'axe de l'Exhaustivité de la vision.

- Le fournisseur doit vendre et supporter activement ses produits de sauvegarde et de récupération sous sa propre marque dans au moins trois des principales zones géographiques suivantes : Amérique du Nord, EMEA, Asie/Pacific et Amérique du Sud. Au moins 25 % du chiffre d'affaires total doit provenir de l'extérieur de sa zone géographique principale.

- Le fournisseur doit servir une base installée d'au moins 1 000 clients sur le marché, tel que défini dans la section Définition/Description du marché. En outre, au moins 250 des 1 000 clients doivent avoir déployé la solution de sauvegarde pour un minimum de 100 serveurs physiques ou 300 serveurs virtuels dans un site de déploiement unique ou une région sur le cloud. Cela exclut les sauvegardes de endpoint.

- Le produit doit être installé dans au moins trois des principales zones géographiques suivantes (Amérique du Nord, EMEA, Asie/Pacifique et Amérique du Sud). Le Fournisseur fournira la preuve d'un minimum de 50 clients de production ayant généré des revenus dans chacune des trois zones géographiques.

- Le fournisseur doit employer au moins 100 collaborateurs à temps plein aux fonctions combinées d'ingénierie, de vente et de marketing au 31 mars 2023.

- Le fournisseur doit disposer d'au moins une solution de sauvegarde et de récupération qualifiante disponible commercialement pour les entreprises pendant trois années civiles avant le 1er mars 2023, c'est-à-dire qu'elle doit avoir été disponible commercialement au moins dès le 1er mars 2020.

- Le produit peut être vendu en tant qu'offre logicielle uniquement, en tant qu'appliance de stockage de sauvegarde virtualisée ou intégrée (application de sauvegarde et stockage de

sauvegarde dans une offre intégrée unique) ou en tant qu'offre de sauvegarde en tant que service (BaaS) développée par un fournisseur et basée sur une offre SaaS.

Les critères d'exclusion suivants s'appliquent :

- Fournisseurs proposant des produits ou solutions avec des logiciels principalement externalisés auprès d'un ISV tiers.
- Produits qui servent uniquement de cible ou de destination pour la sauvegarde, mais qui n'exécutent pas réellement la fonction de gestion de sauvegarde et de restauration. Les exemples comprennent les appliances de déduplication conçues sur mesure, SAN (storage area network), NAS ou le stockage d'objets.
- Fournisseurs qui effectuent des sauvegardes directement sur le cloud public sans stocker de copie locale sur site.
- Les fournisseurs dont la principale source de revenus de produits (plus de 75 % du revenu total) provient des hébergeurs de centres de données et des fournisseurs de services gérés.
- Produits ou solutions conçus et positionnés principalement comme solutions de sauvegarde des endpoints comme les ordinateurs portables, les ordinateurs de bureau et les appareils mobiles.
- Produits ou solutions conçus et positionnés principalement comme des solutions de sauvegarde des applications SaaS.
- Produits ou solutions conçus et positionnés principalement comme solutions de sauvegarde des bureaux distants, des sites Edge et des environnements du marché intermédiaire inférieur/PME.
- Produits ou solutions conçus et positionnés principalement comme des solutions pour des environnements homogènes – comme des outils conçus pour sauvegarder uniquement AWS EC2, Azure Virtual Machines, Microsoft Hyper-V, VMware, Red Hat ou des conteneurs.
- Produits ou solutions conçus pour sauvegarder des fournisseurs de systèmes de stockage ou hyperconvergés spécifiques.
- Les produits qui servent uniquement d'outils de réplication et de reprise après sinistre.
- Produits qui servent essentiellement à gérer les capacités d'instantané et de réplication des baies de stockage.
- Produits principalement positionnés pour la gestion des données de copie (CDM) ou les tests DevOps.
- Produits positionnés principalement en tant que solutions de protection continue des données (CDP).

Critères d’évaluation

Capacité d’exécution

Tableau 1 : Critères d’évaluation de la capacité d’exécution

Critères d’évaluation	*Coefficient*
Produit ou service	Élevée
Viabilité globale	Élevée
Exécution commerciale/tarification	Moyenne
Réactivité sur le marché/antécédents	Élevée
Exécution marketing	Faible
Expérience client	Élevée
Opérations	Non évaluées

Source : Gartner (août 2023)

Exhaustivité de la vision

Tableau 2 : Critères d’évaluation de l’exhaustivité de la vision

Critères d’évaluation	*Coefficient*
Compréhension du marché	Élevée
Stratégie marketing	Moyenne

Critères d’évaluation	*Coefficient*
Stratégie commerciale	Moyenne
Stratégie de l’offre (produit)	Élevée
Modèle commercial	Moyenne
Stratégie verticale/sectorielle	Moyenne
Innovation	Élevée
Stratégie géographique	Moyenne

Source : Gartner (août 2023)

Descriptions des Quadrants

Leaders

Les Leaders présentent les mesures combinées les plus élevées en termes de Capacité d’exécution et d’Exhaustivité de la vision. Ils disposent des portefeuilles de produits les plus complets et évolutifs pour prendre en charge les exigences de protection des données des environnements informatiques hybrides et multicloud. Ils ont fait leurs preuves en matière de présence établie sur le marché et de performances financières. En ce qui concerne leur vision, ils sont perçus dans l’industrie comme des leaders d’opinion et des créateurs de propriété intellectuelle (PI), et ont des plans parfaitement structurés pour améliorer les capacités de récupération, améliorer la facilité de déploiement et d’administration, et augmenter leur évolutivité et l’étendue de leurs produits. Un principe fondamental des Leaders est leur capacité à articuler la manière dont les nouvelles exigences seront prises en charge dans le cadre de leur vision de la gestion de la reprise.

En tant que groupe, on peut s’attendre à ce que les Leaders soient envisagés dans la plupart des nouvelles propositions d’achat et à ce qu’ils aient des taux de réussite élevés pour remporter de nouveaux marchés. Cependant, une part de marché importante n’est pas, à elle seule, un indicateur principal d’un Leader. Les leaders sont des fournisseurs stratégiques qui sont bien

positionnés pour l'avenir, ayant réussi à répondre aux besoins des centres de données des moyennes et grandes entreprises.

Challengers

S'il peuvent exécuter aujourd'hui, les Challengers peuvent toutefois avoir une vision plus limitée que les Leaders, ou doivent encore produire ou commercialiser pleinement leur vision. Ils ont des produits fiables et peuvent être bien adaptés à de nombreuses entreprises. Ces fournisseurs disposent des ressources financières et commerciales et des capacités pour devenir potentiellement des Leaders. Pourtant, la question importante est de savoir s'ils comprennent les tendances et les exigences du marché pour réussir demain, et s'ils peuvent maintenir leur dynamique en exécutant à un niveau élevé sur le long terme.

Un Challenger peut avoir un portefeuille de sauvegarde robuste. Pour autant, il peut ne pas avoir pu se montrer capable de tirer pleinement parti de ses opportunités ou sans avoir la même capacité que les Leaders à influencer les attentes des utilisateurs finaux et/ou à être envisagés pour des déploiements sensiblement plus nombreux ou plus larges. Les Challengers peuvent ne pas être en mesure de rivaliser de manière agressive en dehors de leur base de comptes existante et peuvent se concentrer principalement sur la fidélisation. Ces fournisseurs peuvent ne pas consacrer suffisamment de ressources au développement de produits présentant de l'attrait pour l'ensemble du secteur et des fonctionnalités différenciées en temps opportun. Ils peuvent ne pas commercialiser efficacement leurs capacités et/ou exploiter pleinement suffisamment de ressources sur le terrain pour obtenir une plus grande présence sur le marché.

Visionnaires

Les Visionnaires sont tournés vers l'avenir, font progresser les capacités de leur portefeuille en avance, ou largement en avance sur le marché, mais leur exécution globale ne leur a pas permis de devenir des Challengers ou des Leaders. Cela est souvent dû à des ventes et à un marketing limités, et parfois à l'évolutivité, à l'étendue des charges de travail protégées ou encore à l'étendue des fonctionnalités et/ou de la prise en charge de la plateforme. Ces fournisseurs sont principalement différenciés par l'innovation produit et les avantages perçus par les clients. Cependant, ils n'ont pas encore atteint une solution complète ou n'ont pas encore soutenu les ventes et le marketing à grande échelle. Ils n'ont pas réussi à partager l'esprit ni démontré les déploiements réussis continus dans les grandes entreprises nécessaires pour leur donner la plus grande visibilité des Leaders.

Certains fournisseurs sortent du quadrant des Visionnaires pour entrer dans le quadrant des Acteurs de niche, car leur technologie n'est plus visionnaire (la concurrence les a rattrapés). Dans certains cas, ils n'ont pas été en mesure d'établir une présence sur le marché qui justifierait l'accès aux quadrants des Challengers ou Leaders, voire de rester dans le quadrant des Visionnaires.

Acteurs de niche

Il est important de noter que Gartner ne recommande pas d'éliminer les Acteurs de niche des évaluations des clients. Les Acteurs de niche se concentrent spécifiquement et consciemment

sur un sous-segment du marché global, ou proposent des capacités relativement larges sans échelle de très grande entreprise ou sans le succès global des concurrents d'autres quadrants. Dans plusieurs cas, les Acteurs de niche sont très forts dans le segment des entreprises de taille moyenne supérieure. Ils vendent également de manière opportuniste aux grandes entreprises, mais avec des offres et des services généraux qui, à l'heure actuelle, ne sont pas aussi complets que ceux d'autres fournisseurs axés sur le marché des grandes entreprises.

Les Acteurs de niche peuvent se concentrer sur des zones géographiques, des marchés verticaux spécifiques, ou un déploiement de sauvegarde ou un service de cas d'utilisation ciblé ; ou ils peuvent simplement avoir des horizons modestes et/ou des capacités globales inférieures par rapport aux concurrents. D'autres Acteurs de niche sont trop nouveaux sur le marché ou ont pris du retard, et, bien qu'ils méritent d'être pris en compte, ils n'ont pas encore complètement développé une fonctionnalité complète ou démontré de manière constante une vision étendue ou la Capacité d'exécution.

Contexte

Les responsables de l'infrastructure et des opérations (I&O) chargés des opérations de sauvegarde doivent évaluer et repenser l'infrastructure de sauvegarde de manière à inclure les aspects suivants de la technologie, des opérations et de la consommation :

- Investissez dans des solutions de sauvegarde qui répondent aux exigences de protection des données dans les environnements de centre de données, hybride, multicloud et de périphérie. Favorisez les solutions qui offrent une vue unifiée pour la gestion de ces environnements distribués.

- Choisissez des solutions de sauvegarde qui fournissent une offre intégrée ou intégrée pour protéger les données de sauvegarde contre les attaques par ransomware, la détection des anomalies dues à des ransomwares et des logiciels malveillants, ainsi que des capacités de récupération accélérée après une attaque par ransomware.

- Afin de garantir la résilience de la sauvegarde, comprenez parfaitement le niveau de résilience fourni sur la copie de sauvegarde principale et la nécessité d'investir dans des copies de sauvegarde supplémentaires, comme le cloud, prise en charge du verrouillage d'objet, coffres-forts de données immuables ou bande.

- Choisissez des produits qui offrent des capacités de test de récupération sécurisée et granulaire.

- Alignez l'architecture de sauvegarde sur les besoins de récupération opérationnelle de leur organisation. Optimisez l'utilisation du stockage de sauvegarde en utilisant un stockage sur disque tel que des appliances de sauvegarde spécialement conçues ou un système de fichiers distribué, un stockage objet ou SAN pour la récupération opérationnelle, et l'utilisation de bandes sur site, de stockage objet ou de cloud public ou hébergé par un fournisseur stockage pour la conservation à long terme et les copies à vide d'air.

- Déterminez le coût total d'acquisition à long terme du passage des licences perpétuelles aux modèles de licences par abonnement. Pour les abonnements, comprenez les implications financières des paiements annualisés par rapport aux paiements initiaux, et de la résiliation de l'abonnement avant la fin de la période.

- Comprendre les implications financières à long terme des différents modèles de tarification proposés par les fournisseurs - basés sur les VM, les sockets, les nœuds, l'universel, le front-end TB, le back-end TB et les agents. Investissez dans le modèle adéquat d'après la feuille de route de l'application et de l'infrastructure de l'organisation.

- Choisissez des fournisseurs qui prennent en charge la hiérarchisation des copies de sauvegarde vers le cloud public et dans le cloud public afin de réduire les coûts de stockage en sauvegarde. Choisissez des solutions prenant en charge la récupération d'applications à partir de copies de sauvegarde dans le cloud public de manière à satisfaire les cas d'utilisation de reprise après attaque par ransomware, de test/développement ou DR.

- Sélectionnez des fournisseurs capables d'accroître la valeur des données de sauvegarde au-delà des événements de récupération. Donnez la priorité aux solutions qui comprennent une analyse des données sensibles et une e-découverte, répondent aux exigences de conformité, prennent en charge l'analytique et d'autres enrichissements de données, réutilisent les données de sauvegarde pour les tests/développement et fournissent des capacités complémentaires comme la reprise après sinistre.

Vue d'ensemble du marché

Le marché des logiciels de sauvegarde et de récupération pour entreprise a connu une transformation significative au cours des deux dernières années. Les fournisseurs de sauvegarde évalués dans ce Magic Quadrant se sont principalement focalisés sur les domaines suivants :

- **Plan de contrôle centralisé :** Alors que les entreprises évoluent vers un modèle informatique hybride et multicloud, et que les charges de travail sont distribuées dans le centre de données, le cloud public et la périphérie, la protection de ces charges de travail, quel qu'en soit l'emplacement, est essentielle. Les principaux fournisseurs de solutions de sauvegarde s'attaquent à ce problème en proposant une plateforme de gestion qui peut être déployée dans le cloud public, dans le centre de données principal ou, de plus en plus, en tant que service hébergé dans le cloud public.

- **Protection multicloud :** alors que les organisations déploient des applications et des charges de travail dans plusieurs environnements cloud, l'exigence de solutions pour intégrer et protéger les environnements multicloud est désormais plus critique. Choisir le fournisseur de cloud utilisé pour stocker les données de sauvegarde offre une flexibilité idéale.

- **Résilience face aux attaques par ransomware :** L'augmentation du nombre d'attaques par ransomware a conduit les fournisseurs à prendre des mesures concrètes afin de progresser vers une infrastructure de sauvegarde résiliente. La plupart des fournisseurs s'efforcent de rendre le référentiel de sauvegarde principal plus résilient en prenant en charge le stockage immuable pour les premières copies. Alors que la plupart des fournisseurs prennent en charge

la création de deuxièmes copies immuables de sauvegarde par écriture une fois, le stockage compatible avec la technique Write Once Read Many (WORM), comme le verrouillage du stockage d'objets, les principaux fournisseurs de sauvegarde ont introduit des coffres-forts de données immuables sur site, dans le cloud et hébergés par les fournisseurs.

- **Détection et correction après attaque par ransomware** : les principaux fournisseurs ont développé des capacités pour détecter les attaques par ransomware en surveillant les anomalies comportementales des données protégées et ajoutent la détection des logiciels malveillants fournie par un partenariat avec des fournisseurs de sécurité ou en développant ces capacités en interne. La plupart des fournisseurs visent également à simplifier le processus de récupération après attaque par ransomware en accélérant l'identification du meilleur point de récupération et du point le plus propre en créant des points de récupération organisés, combinant plusieurs points de récupération et en créant un environnement de test et de récupération isolé.

- **Offres BaaS** : Les principaux fournisseurs de sauvegarde étendent les capacités BaaS pour inclure les environnements sur site, IaaS, PaaS et SaaS. Bien qu'ils ne remplacent généralement pas les déploiements de sauvegarde sur site, les clients de Gartner investissent dans des offres BaaS pour compléter ces déploiements afin de simplifier la protection des environnements, y compris les charges de travail sur site sélectionnées et le cloud Edge et public.

- **Utilisation de l'intelligence artificielle et du machine learning** : les principaux fournisseurs ont introduit des algorithmes basés sur l'IA/le ML dans les capacités de détection des anomalies dues à des ransomware, ainsi que pour améliorer les pratiques en matière de support client. Les nouvelles fonctionnalités comprennent des avancées dans la classification automatisée des données et les activités administratives basées sur la conversation.

- **Prise en charge de la sauvegarde IaaS et PaaS sur le cloud public** : les principaux fournisseurs de sauvegarde sur site ont augmenté leur investissement afin de créer des capacités visant à protéger les charges de travail natives sur le cloud, en particulier les machines virtuelles et les applications hébergées dans AWS, Microsoft Azure et Google Cloud Platform. Les principaux fournisseurs de sauvegarde développent également le soutien à la sauvegarde des produits DBaaS, tels qu'Amazon RDS, Amazon Aurora et Microsoft Azure SQL. Certains fournisseurs intègrent le logiciel de sauvegarde dans les capacités natives de snapshot offertes par ces fournisseurs de cloud ; d'autres continuent à réutiliser leur logiciel de sauvegarde existant « tel quel » dans le cloud afin de fournir une sauvegarde basée sur agent des applications hébergées dans le cloud.

- **Prise en charge des applications SaaS** : Les responsables I&O ont commencé à inclure des applications SaaS comme Microsoft 365, Google G Suite et Salesforce dans leur stratégie de sauvegarde. La plupart des fournisseurs évalués dans cette étude fournissent une sauvegarde Microsoft 365 et Salesforce par l'intermédiaire de partenaires ou ont développé ces capacités en interne. Les principaux fournisseurs protègent d'autres applications SaaS comme Microsoft

Azure Active Directory, Microsoft Dynamics 365, Microsoft Power Apps, Atlassian et ServiceNow.

- **Hiérarchisation sur le cloud public** : La plupart des fournisseurs évalués dans ce Magic Quadrant prennent en charge la hiérarchisation des données de sauvegarde sur le cloud public. Cela réduit les coûts de stockage de sauvegarde sur site. Les cibles de stockage sur cloud public les plus couramment prises en charge sont Amazon Simple Storage Service (Amazon S3) et Azure Blob. Dans la plupart des cas, les données de sauvegarde sont auto-descriptives, ce qui signifie qu'en cas de perte des données et du catalogue sur site, une instance du logiciel de sauvegarde peut être réinstallée dans le cloud et les données peuvent être restaurées. Certains fournisseurs s'intègrent également dans les politiques de cycle de vie des fournisseurs de cloud (par exemple, migration de données d'Amazon S3 vers Glacier, ou stockage Azure Blob vers Azure Archive Blob).

- **Récupération dans le cloud public** : Aujourd'hui, les principaux fournisseurs de sauvegarde prennent en charge la restauration des données de sauvegarde sur les serveurs du cloud public. Une instance du logiciel de sauvegarde peut être installée dans le cloud public, et les données de sauvegarde peuvent être restaurées sur une instance informatique dans le cloud public. Cela permet une récupération opérationnelle rapide en cas d'indisponibilité de l'environnement sur site. Les données de sauvegarde peuvent également être utilisées à des fins de test/développement dans le cloud public.

- **Sauvegarde de base de données NoSQL** : Les entreprises traditionnelles continuent d'exécuter leurs principales applications métier sur les bases de données de système de gestion de base de données relationnelle (RDMS) telles qu'Oracle et Microsoft SQL. Cependant, les projets de Mode 2 comme le Big Data exploitent généralement les bases de données NoSQL comme MongoDB et Cassandra. Alors que ces projets commencent à évoluer et à fournir une valeur tangible, un besoin croissant de protéger ces environnements se fait sentir. Des fournisseurs établis comme Commvault, Dell et Veritas Technologies ont commencé à répondre à ces exigences de sauvegarde en intégrant ces capacités de manière native dans la plateforme de sauvegarde. Des fournisseurs comme Rubrik et Cohesity ont effectué des rachats stratégiques dans ce domaine.

- **Récupération instantanée des bases de données, des machines virtuelles et des systèmes de fichiers** : La majeure partie des fournisseurs prend en charge la récupération instantanée des machines virtuelles en installant la machine virtuelle sauvegardée directement sur l'hôte de production via NFS. Les machines virtuelles peuvent ainsi devenir instantanément disponibles, alors que le processus de récupération réel peut être initié en arrière-plan. Des fournisseurs comme Cohesity et Rubrik offrent une récupération instantanée de bases de données comme Microsoft SQL et Oracle, tandis que Veeam offre également un accès ponctuel au partage de fichiers à partir de sauvegardes via un partage de fichiers SMB en lecture seule.

- **Sauvegarde en conteneur** : Les principaux fournisseurs ont annoncé leur prise en charge de la sauvegarde en conteneur, soit en construisant ces capacités de manière native dans leur plateforme existante, soit par le biais d'acquisitions. Bien que les demandes d'informations des

clients de Gartner indiquent un faible intérêt pour la sauvegarde en conteneur, nous prévoyons une augmentation de son adoption, dans la mesure où davantage de conteneurs utilisant le stockage persistant sont déployés pour prendre en charge les charges de travail de production.
- **Modèles de licences :** Bien que certaines options de licences perpétuelles restent disponibles, tous les principaux fournisseurs de ce marché sont passés à la fourniture de leurs offres logicielles par le biais de modèles de licences par abonnement. La plupart des offres de licence basée sur abonnement sont des accords sur plusieurs années. La licence basée sur la consommation constitue une tendance émergente à la licence qui offre la possibilité de concéder sous licence ce qui est utilisé en fonction de la mesure à des intervalles plus fréquents.

Définitions des critères d'évaluation

Capacité d'exécution

Produit/Service : produits et services de base proposés par le fournisseur pour le marché défini. Cela inclut entre autres les fonctionnalités des produits et services actuels, la qualité, les ensembles de fonctionnalités et les compétences, qu'elles soient proposées de manière native ou par l'intermédiaire d'accords/de partenariats OEM, comme précisés dans la définition du marché et détaillés dans les critères secondaires.

Produit/Service : produits et services de base proposés par le fournisseur pour le marché défini. Cela inclut entre autres les fonctionnalités des produits et services actuels, la qualité, les ensembles de fonctionnalités et les compétences, qu'elles soient proposées de manière native ou par l'intermédiaire d'accords/de partenariats OEM, comme précisés dans la définition du marché et détaillés dans les critères secondaires.

Exécution commerciale/tarification : les capacités d'un fournisseur dans toutes les activités préliminaires à la vente et au sein de la structure soutenant ces activités. Il s'agit notamment de la gestion des transactions de vente, de la tarification et de la négociation, du support technique préliminaire à la vente et de l'efficacité globale du circuit de distribution.

Réactivité sur le marché/antécédents : aptitude à réagir, à changer de direction, à faire preuve de souplesse et à réussir face à la concurrence au fur et à mesure que des opportunités surgissent, que les concurrents agissent, que les besoins des clients évoluent et que la dynamique du marché change. Ce critère tient également compte de la réactivité du fournisseur par le passé.

Exécution marketing : la clarté, la qualité, la créativité et l'efficacité des programmes conçus pour transmettre le message de l'organisation afin d'influencer le marché, de promouvoir la marque et l'entreprise, de sensibiliser le marché aux produits proposés et d'aider les acheteurs potentiels à percevoir le produit/la marque et l'organisation de façon positive. Cette « notoriété » peut être issue d'une combinaison d'actions publicitaires, d'initiatives promotionnelles, de décisions stratégiques éclairées, du bouche-à-oreille et d'activités commerciales.

Expérience client : relations, produits, services et programmes permettant aux clients de réussir avec les produits évalués. Cet aspect comprend spécifiquement la façon dont les clients reçoivent un support technique ou client. Il peut également tenir compte des outils auxiliaires, des

programmes de support client (et de leur qualité), de la disponibilité de groupes d'utilisateurs, des accords de niveaux de service (accords de niveaux de services), etc.

Opérations : aptitude d'une organisation à atteindre ses objectifs et à respecter ses engagements. Parmi les facteurs étudiés figure la qualité de la structure organisationnelle, notamment les compétences, les expériences, les programmes, les systèmes et tous les autres moyens permettant à l'organisation d'exercer ses activités de façon toujours efficace et efficiente.

Exhaustivité de la vision

Compréhension du marché : aptitude du fournisseur à comprendre les désirs et les besoins des acheteurs, et à concrétiser leurs aspirations en produits et services. Les fournisseurs dont la vision est complète sont à l'écoute des acheteurs et savent comprendre leurs désirs et leurs besoins. Ils peuvent ainsi façonner ou rehausser leurs attentes grâce à leur vision.

Stratégie marketing : ensemble de messages clairs et différenciés qui sont communiqués avec cohérence dans toute l'organisation et à l'extérieur par le biais d'un site Web, de messages publicitaires, de programmes destinés aux clients et de déclarations de positionnement.

Stratégie commerciale : stratégie permettant de vendre des produits par le biais d'un réseau approprié d'affiliés directs et indirects travaillant dans les domaines de la vente, du marketing, du service et de la communication. Cela permet à l'organisation d'étendre sa portée, de pénétrer le marché en profondeur et d'augmenter ses compétences, son savoir-faire, ses technologies, ses services et le nombre de ses clients.

Stratégie de produit : approche du fournisseur pour le développement et la distribution de ses produits. Cette stratégie doit mettre en valeur la différenciation, les fonctionnalités, la méthodologie et les caractéristiques en fonction des besoins actuels et futurs.

Modèle commercial : bien-fondé et logique de la proposition commerciale de base du fournisseur.

Stratégie verticale/sectorielle : stratégie du fournisseur pour concentrer ses ressources, ses compétences et ses produits afin de répondre aux besoins spécifiques d'un segment de marché précis, y compris pour les marchés verticaux.

Innovation : allocation directe, connexe, complémentaire et synergique de ressources, d'expertise ou de fonds à des fins d'investissement, de consolidation, de défense ou de prévention.

Stratégie géographique : stratégie du fournisseur pour cibler ses ressources, ses compétences et ses produits en fonction des besoins précis de régions géographiques en dehors du territoire initial, que ce soit de façon directe ou par le biais de partenaires, de canaux et de filiales implantés dans ces autres territoires et marchés.

L'étude de Gartner contenue dans ce document a été traduite de la version originale anglaise dans la langue ci-dessus/dans le document. Gartner a déployé tous les efforts professionnels raisonnables pour assurer que la traduction soit aussi exacte et complète que possible. Toutefois, comme pour toute traduction, il peut inévitablement y avoir un certain degré de divergence. En cas de divergence de contenu ou d'intention, la signification de la version originale anglaise prévaudra toujours.