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

5 août 2024 - ID G00800390 - 45 min de lecture

Par les analystes : Michael Hoeck, Jason Donham, Rene Rodriguez, Chandra Mukhyala

La protection des applications et des données vitales de l'entreprise des multiples menaces et leur récupération est un défi majeur pour les responsables I&O. Le marché des solutions logicielles de sauvegarde et de récupération d'entreprise répond à ce besoin par une couverture plus large des charges de travail, des fonctionnalités de récupération post-ransomware et des modèles de mise en œuvre axés sur la simplicité.

Hypothèses de planification stratégique

- D'ici 2028, 75 % des entreprises utiliseront une solution commune de sauvegarde et de récupération des données hébergées sur site et dans l'infrastructure cloud, contre 20 % en 2024.
- D'ici 2028, 75 % des entreprises considèreront la sauvegarde des applications SaaS comme une exigence majeure, contre 15 % en 2024.
- D'ici 2028, 90 % des produits de sauvegarde et de récupération pour l'entreprise comprendront une technologie intégrée de détection et d'identification des cybermenaces, contre moins de 45 % en 2024.
- D'ici 2028, 75 % des grandes entreprises adopteront la sauvegarde en tant que service (BaaS), parallèlement aux outils sur site, pour la sauvegarde des charges de travail cloud et sur site, contre 15 % en 2024.
- D'ici 2028, 75 % des produits de sauvegarde et de récupération d'entreprise intégreront l'IA générative pour améliorer leurs opérations de gestion et de support, contre moins de 5 % en 2024.

Définition/description du marché

Gartner définit les solutions logicielles de sauvegarde et de récupération d'entreprise comme une technologie effectuant une copie ponctuelle (sauvegarde) des données de l'entreprise dans les environnements sur site, hybrides, multicloud et logiciels en tant que service (SaaS). Ces solutions

enregistrent ces données sur un ou plusieurs support(s) de stockage secondaire(s), essentiellement à des fins de récupération en cas de perte.

La protection et la récupération des données des applications métier, quel que soit le type d'infrastructure sous-jacente et son emplacement, sont plus importantes que jamais. Les entreprises évoluant vers des environnements de plus en complexes, aux volumes de données vitales importants et étendus, les solutions logicielles de sauvegarde et de récupération pour l'entreprise protègent ces charges de travail quel que soit leur environnement de résidence - sur site, hybrides, multicloud ou SaaS.

Ces solutions sont essentielles pour permettre aux entreprises de récupérer leurs données suite à un événement ayant rendues celles-ci inaccessibles. Que cet événement soit accidentel, malveillant ou lié à leur environnement, les entreprises utilisent ces solutions pour récupérer et restaurer l'accès à leurs données affectées avec précision et efficacité.

Ces solutions doivent offrir des fonctionnalités efficaces, simplifiant la gestion de la protection des données dans les environnements d'entreprise complexes. Elles doivent aussi garantir une récupération fiable suite à des erreurs accidentelles ou opérationnelles, mais aussi à des pertes de données résultant de menaces en constante évolution. Enfin, ces solutions doivent accélérer et orchestrer la récupération des données et la reprise après sinistre ou attaque par ransomware classiques.

Fonctionnalités indispensables

Les solutions logicielles de sauvegarde et de récupération pour l'entreprise doivent impérativement comprendre les fonctionnalités suivantes :

- Sauvegarde des données et des systèmes dans des environnements multicloud hybrides et sur site. Sur site, ces solutions doivent assurer la protection des systèmes d'exploitation, des fichiers, des bases de données, des machines virtuelles et des applications. Pour le cloud, les fonctionnalités indispensables sont la protection de l'infrastructure en tant que service (IaaS), de la plateforme en tant que service (PaaS), de la base de données en tant que service (DBaaS) et du SaaS.
- Récupération de données et de systèmes suite à une défaillance ou à une perte de données, comme une défaillance opérationnelle, système ou d'application, une erreur accidentelle, une catastrophe naturelle ou une cyberattaque. Ces récupérations nécessitent des fonctionnalités de mise en œuvre de politiques de sauvegarde et de gestion des données répondant aux besoins de l'entreprise en matière d'objectifs de points de récupération (RPO), de temps de récupération (RTO), de résilience, de cycle de vie des données et de conformité.
- Intégration de supports de stockage de sauvegarde immuables ou mise en œuvre de stockage immuable fourni par le fournisseur.

Fonctionnalités standard

Les fonctionnalités standard des solutions logicielles de sauvegarde et de récupération comprennent :

- La protection des données vitales des applications SaaS ou PaaS, comme Google Workspace, Microsoft 365, Microsoft Entra ID, les applications Salesforce et d'autres sources, y compris le stockage d'objets et les conteneurs.
- Une console centralisée pour la gestion de l'infrastructure de solutions de sauvegarde distribuées dans les environnements hybrides et multicloud.
- Des fonctionnalités de sécurité avancées, comme l'intégration de solutions de gestion des accès privilégiés, l'authentification multifacteur, les contrôles d'accès basés sur les rôles et la validation des modifications multipersonnes, la gestion des informations et des événements de sécurité (SIEM) et l'orchestration de la sécurité, l'intégration de l'automatisation et de la réponse (SOAR), et le reporting et la journalisation de sécurité avancés.
- Des fonctionnalités avancées de préparation à la cyber-récupération, comme la détection intégrée d'anomalies et d'entropies développée par le fournisseur ou par un tiers, la détection de logiciels malveillants et de signatures, ainsi que des offres d'environnements de récupération isolés et de coffres-forts de données immuables.
- L'orchestration des tests et processus de reprise après sinistre et de cyber-récupération.

Fonctionnalités optionnelles

Les autres fonctionnalités proposées par les solutions logicielles de sauvegarde et de récupération pour l'entreprise sont :

- La protection de charges de travail supplémentaires et prise en charge de cas d'utilisation comme les sites distants/périphériques, les terminaux et l'infrastructure et les données LLM (Large Language Model).
- Un plan de contrôle SaaS hébergé par le fournisseur pour la gestion et l'orchestration des environnements complexes et distribués.
- Une offre de sauvegarde en tant que service (BaaS) hébergée par le fournisseur : services de sauvegarde et de récupération pour les environnements hybrides et multicloud.
- Des fonctionnalités d'IA générative simplifiant l'administration, améliorant les services d'assistance et accélérant les procédures de sauvegarde et de récupération.
- La prise en charge de cas d'utilisation de sauvegarde de données étendus, facilitant la découverte des données, la sécurité, la conformité, la gestion des données de copie, les tests et le développement, ainsi que les processus de découverte électronique.

Magic Quadrant

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

Points forts et mises en garde à l'égard des fournisseurs

Arcserve

Arcserve est l'un des Acteurs de niche de ce Magic Quadrant. Le portefeuille de sauvegarde d'Arcserve comprend Arcserve Unified Data Protection (UDP), Arcserve Backup, les applications matérielles Arcserve série 9000, Arcserve UDP Cloud Hybrid et les applications matérielles de stockage Arcserve OneXafe et Arcserve SaaS Backup. Les opérations d'Arcserve sont géographiquement diversifiées, la majeure partie de ses clients se trouvant dans le segment du marché intermédiaire. Au cours de la période d'évaluation, Arcserve a lancé UDP 9.1 et 9.2, améliorant la sécurité des mots de passe pour les opérations de sauvegarde et de récupération,

les opérations de devises par de nouvelles distributions Linux, des correctifs de sécurité et la sécurisation avancée de la base de données SQL Express.

Points forts

- **Options de tarification souples :** Arcserve offre à ses clients le choix entre une licence d'abonnement perpétuelle et à durée déterminée, ainsi que plusieurs statistiques, dont par téraoctet front-end, par socket et par machine virtuelle, afin d'optimiser la tarification en fonction de leurs besoins.

- **Protection complète des applications SaaS :** grâce à sa relation OEM avec Keepit, Arcserve SaaS Backup fournit la protection de Microsoft 365, Salesforce, Microsoft Entra ID, Google Workspace, Zendesk, Microsoft Power BI et Azure DevOps.

- **Couverture géographique :** la stratégie géographique très complète d'Arcserve comprend des gestionnaires territoriaux, des revendeurs à valeur ajoutée (VAR) et des prestataires de services gérés (MSP) dans toutes les grandes régions du monde.

Réserves

- **Une expérience client qui affecte l'innovation :** principalement axé sur la résolution des problèmes liés au renforcement de ses solutions, de son assistance client et de son expérience clients potentiels et les investissements en résultant, Arcserve n'a que peu innové en matière de sauvegarde et de restauration, tendance actuelle du marché.

- **Une utilisation tardive de l'IA :** le portefeuille actuel et la roadmap à court terme d'Arcserve n'offrent pas la mise en œuvre de l'IA dans des domaines comme la détection des anomalies liées à un ransomware, la cyber-récupération avancée et les cas d'utilisation de l'IA générative.

- **Une protection cloud native basée sur les agents :** les offres d'Arcserve restent fortement tributaires de la sauvegarde basée sur les agents pour la protection des charges de travail cloud natives, comme la plateforme en tant que service (PaaS) et l'infrastructure en tant que service (IaaS), ce qui complique l'administration du déploiement et la gestion de ces environnements cloud.

Cohesity

Cohesity est l'un des Leaders de ce Magic Quadrant. Son portefeuille de sauvegarde DataProtect est disponible pour un déploiement géré par le client, sur site et dans le cloud ou comme offre en tant que service. Couvrant principalement l'Amérique du Nord et l'Europe occidentale, Cohesity est peu présent en Asie/Pacifique et en Amérique latine. Ses clients se situent généralement dans les segments supérieurs du marché intermédiaire et des entreprises. L'un de ses nouveaux produits majeurs présentés durant la période d'évaluation est Cohesity Gaia, une solution de recherche et de réponse conversationnelle basée sur l'IA générative et alimentée par des données de sauvegarde. Cohesity offre de nouvelles fonctionnalités d'IA améliorant la détection des menaces et guidant l'opérateur dans la cyber-récupération, l'administration et le dépannage des problèmes liés aux produits. Ses autres améliorations notables sont la personnalisation des règles d'analyse des menaces, la classification des données à la demande, la prise en charge des machines

virtuelles (VM) Azure, Azure SQL, Amazon RDS pour PostgreSQL, Amazon Aurora, VMware Cloud on Amazon Web Services (AWS) et la récupération instantanée des machines virtuelles Nutanix AHV.

En février 2024, Cohesity a annoncé l'acquisition des actifs de protection des données Veritas NetBackup et Alta, dont la finalisation est prévue d'ici la fin de l'année. Cette opération est la plus importante fusion/acquisition du marché depuis plus d'une décennie. Le portefeuille complet de sauvegarde et de restauration de la société comprendra des technologies complémentaires et se recoupant.

Points forts

- **Innovation et exécution :** depuis sa création, Cohesity ne cesse d'innover en matière de protection, de sécurité et de gestion des données, ainsi que la fourniture en-tant-que-service pour les données sur site, cloud et SaaS.
- **L'IA générative pour les données de l'entreprise :** Cohesity est le premier fournisseur à proposer une solution basée sur l'IA générative, alimentée par le référentiel de données de sauvegarde et offrant une solution conversationnelle en langage naturel, répondant aux questions des entreprises.
- **Le Marketplace de Cohesity :** Cohesity propose de nombreuses applications natives et tierces à valeur ajoutée sur son Marketplace, ne se limitant pas à la simple sauvegarde, mais analysant les données de celle-ci.

Réserves

- **Couverture limitée des applications SaaS :** le portefeuille d'applications SaaS de Cohesity reste limité, à l'exception de Microsoft 365 et Salesforce.
- **Absence de logiciel de sauvegarde autonome :** la solution de Cohesity est une offre complète de logiciels de sauvegarde et de stockage. Elle ne comprend pas la sauvegarde seule, enregistrant la première copie sur un support de stockage tiers.
- **Intégration de Veritas :** la finalisation de l'acquisition par Cohesity des opérations de protection des données d'entreprise de Veritas risque de mobiliser plusieurs services de la société et de ralentir le rythme d'innovation de Cohesity durant cette phase.

Commvault

Commvault est l'un des Leaders de ce Magic Quadrant. Sa plateforme, Commvault Cloud, comprend des solutions de protection des données, d'analyse des risques et de cyber-récupération des charges de travail sur site et basées sur le cloud/SaaS. Les opérations de Commvault sont géographiquement diversifiées, et ses clients principalement de grandes entreprises. Au cours de la période d'évaluation, Commvault a présenté Arlie, une solution d'analyse des menaces et d'assistant d'opérations basée sur l'IA, ainsi que la détection des menaces par le leurre Threatwise, la détection des logiciels malveillants Threat Scan Predict et Cleanroom Recovery, orchestrant et testant la récupération dans un environnement isolé. En outre,

Commvault a présenté d'autres améliorations d'Oracle Cloud Infrastructure, la prise en charge avancée de la récupération d'ID Microsoft Active Directory et Microsoft Entra, et de la protection des charges de travail MySQL et PostgreSQL dans Azure.

Points forts

- **Prise en charge d'un vaste écosystème** : Commvault est à la fois complet en termes de couverture et de réactivité à l'ajout de nouvelles charges de travail à son offre de sauvegarde et de récupération, Il prend en charge un large éventail de charges de travail d'applications sur site, multicloud et SaaS.

- **Axé sur la cyber-résilience et la récupération** : associé aux intégrations de l'IA d'Arlie et de sécurité tierces, Commvault Cleanroom Recovery simplifie aux clients la planification, la pratique et l'exécution des récupérations complexes.

- **Licence simplifiée** : Commvault a amélioré le système de licences de gestion SKU de ses produits cloud et sur site, à des fins de clarification pour ses clients.

Réserves

- **Problèmes liés au processus d'assistance** : des clients ont fait part de leurs difficultés lors de leurs interactions avec l'équipe d'assistance de Commvault, en termes de réactivité pour faire remonter les incidents au-delà de l'assistance de premier niveau.

- **Difficultés de prise en main par les clients** : certains clients de Gartner indiquent devoir faire appel à l'assistance pour la mise en œuvre de nouvelles fonctionnalités et fonctions. Ils s'interrogent, par conséquent, sur la mise à disposition du grand public (GA) par Commvault de caractéristiques et fonctionnalités sans la fourniture systématique d'une documentation complète pour une mise en œuvre correcte.

- **Confusion liée au changement de nom des produits** : malgré le changement de nom de ses produits (Commvault Cloud), les clients notent une certaine confusion et un manque de clarté et de cohérence des fonctionnalités de Commvault dans ses offres sur site, BaaS et applications matérielles.

Dell Technologies

Dell Technologies est l'un des Leaders de ce Magic Quadrant. Son portefeuille de logiciels de sauvegarde et de récupération comprend PowerProtect Data Manager, PowerProtect Cyber Recovery, CyberSense, NetWorker, Avamar, APEX Backup Services et les applications matérielles des séries PowerProtect DP et DD. Les opérations de Dell sont géographiquement diversifiées, et ses clients principalement de grandes entreprises présentes sur le marché intermédiaire. Les améliorations notables apportées à PowerProtect Data Manager durant la période d'évaluation sont l'intégration de l'agent Storage Direct à Dell PowerStore et Dell PowerMax, la récupération granulaire de Microsoft Active Directory et la prise en charge d'agents autonomes pour Apache Hadoop. À noter également l'intégration de PowerProtect DM5500 à PowerProtect Cyber Recovery, les fonctionnalités des services de sauvegarde APEX (y compris les sauvegardes natives du cloud pour AWS et Azure), le stockage de protection APEX dans Oracle Cloud VMware

Solution et la prise en charge des abonnements APEX pour les applications matérielles de sauvegarde.

Points forts

- **Offre complète de solutions :** Dell a regroupé son portefeuille de serveurs, de stockage, de mise en réseau, ainsi que ses offres de sauvegarde et de récupération en une solution unique réduisant le nombre de fournisseurs nécessaires et améliorant l'expérience client globale.

- **Protection directe du stockage :** les deux solutions PowerMax et PowerStore de Storage Direct Protection comprennent la sauvegarde différentielle par bloc. PowerProtect Data Manager orchestre et gère la sauvegarde et la récupération cohérentes en cas de panne directement depuis et vers les applications matérielles PowerProtect, sans logiciel de sauvegarde à installer sur les systèmes PowerMax et PowerStore.

- **L'abonnement APEX ajoute un support de sauvegarde :** Dell a élargi son offre d'abonnements APEX aux applications matérielles de domaine de données PowerProtect, permettant aux clients d'acquérir des applications matérielles de domaine de données PowerProtect par une licence de paiement à l'utilisation. Un choix qui permet aux clients de commencer petit, de se développer et d'acquérir de nouvelles fonctionnalités selon leurs besoins de performance.

Réserves

- **À la traîne des leaders dans les grandes tendances du marché :** Dell a suivi les leaders du marché en répondant aux tendances récentes de celui-ci, comme les coffres-forts de stockage de sauvegarde cloud hébergés par le fournisseur et les fonctionnalités avancées de détection des ransomware et de récupération, complétant son offre PowerProtect Cyber Recovery.

- **Innovation inégale dans son portefeuille de logiciels de sauvegarde :** principalement axé sur le développement de son offre PowerProtect Data Manager, Dell n'a que peu fait évoluer ses autres produits de sauvegarde et de récupération, comme Avamar et NetWorker.

- **Un plan de contrôle basé sur le SaaS limité :** 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.

Druva

Druva est l'un des Visionnaires de ce Magic Quadrant. Sa plateforme Druva Data Security Cloud est une offre BaaS exploitant l'infrastructure AWS pour l'exécution, le stockage et la gestion des sauvegardes. Cette plateforme se compose de plusieurs produits assurant la sauvegarde et la reprise après sinistre sur site et dans le cloud, la sauvegarde et la reprise après sinistre natives dans le cloud AWS et Kubernetes, et la sauvegarde des applications SaaS et des terminaux. Les opérations de Druva sont géographiquement diversifiées, la majorité de ses clients se situant en Amérique du Nord. Ses clients appartiennent généralement aux segments des moyennes et grandes entreprises. Durant la période d'évaluation, Druva a ajouté la sauvegarde de machines virtuelles Azure, la détection des anomalies des machines virtuelles VMware, la sauvegarde directe à partir de SAP HANA, la récupération Sandbox et les sauvegardes par groupes Microsoft

365. Dru, son copilote IA pour la sauvegarde et la récupération, et la récupération personnalisée des données Microsoft OneDrive et SharePoint Online sont deux autres nouveautés de Druva.

Points forts

- **BaaS cloud natif** : conçue d'emblée comme plateforme cloud native et SaaS, la plateforme BaaS de Druva offre une grande facilité d'utilisation et la mise à l'échelle automatique des ressources pour toutes les données.
- **Entreprises axées sur le cloud** : offrant des versions d'essai en libre-service intégral, une prise en main facilitée et des opérations simplifiées, la plateforme BaaS de Druva convient particulièrement aux entreprises axées sur le cloud.
- **Couverture mondiale avec Dell** : le partenariat OEM de Druva avec Dell Technologies rend son offre disponible dans le monde entier, en tant que solution de marque Dell.

Réserves

- **Déploiements limités à l'échelle de l'entreprise** : par rapport aux Leaders de ce Magic Quadrant, Druva est peu utilisée par les grandes entreprises comme solution unique de protection des données.
- **Prise en charge multicloud moins complète** : la prise en charge par Druva de la sauvegarde des applications et de l'infrastructure dans Azure et Google Cloud Platform (GCP) est limitée par rapport à AWS.
- **Couverture de l'environnement hybride laissant à désirer** : Druva est à la traîne par rapport aux exigences du marché en matière d'environnement hybride, comme la protection des conteneurs, le stockage d'objets et les bases de données modernes, dont MongoDB, MariaDB et NoSQKL, les fonctionnalités de récupération bare-metal et la récupération instantanée des bases de données.

HYCU

HYCU est l'un des Visionnaires de ce Magic Quadrant. HYCU R-Cloud (ex-Protégé) est une plateforme BaaS hybride et multicloud couvrant Azure, AWS et Google pour la prise en charge des charges de travail IaaS, DBaaS (database as a service), PaaS, SaaS et sur site. HYCU R-Graph fournit des informations sur les architectures d'applications et de données dans les environnements sur site, cloud et SaaS. HYCU est surtout présent en Amérique du Nord et dans la région EMEA, la majorité de ses clients se trouvant en Amérique du Nord. Ses clients se situent généralement dans les segments supérieurs du marché intermédiaire. Durant la période d'évaluation, HYCU a présenté plusieurs nouvelles fonctionnalités de R-Graph, dont des options d'affichage personnalisables et des informations sur les fonctionnalités natives de protection des applications. Il a également amélioré R-Cloud, avec la prise en charge d'offres SaaS et PaaS, comme Google Cloud Bigtable, Atlassian Trello, Docusign, GitHub, Amazon DynamoDB, AWS CloudFormation et AWS Key Management Service.

Points forts

- **Prise en charge étendue du cloud :** fortement axé sur les intégrations SaaS et PaaS, HYCU offre la prise en charge d'une longue liste de services généralement absents des autres offres du marché.
- **Meilleure visibilité du parc de protection des données :** R-Graph recueille des données dans l'environnement applicatif des clients et signale les lacunes en matière de protection des données, ce qui leur permet d'identifier facilement leurs actifs non protégés.
- **Intégrations développées par l'IA générative :** HYCU utilise l'IA générative pour accélérer le développement de modules de protection des données des nouvelles charges de travail SaaS et PaaS.

Réserves

- **Limitations sur site :** les versions de produits d'HYCU liées aux besoins sur site, comme AIX, Solaris, SUSE et Ubuntu Linux et la prise en charge des clusters de bases de données, sont à la traîne par rapport aux leaders du marché.
- **Aucune orchestration de la reprise après sinistre :** R-Cloud ne dispose pas de fonctionnalités d'orchestration intégrées simplifiant les opérations de reprise après sinistre et les fonctionnalités de test.
- **Couverture géographique limitée :** la présence et les opérations d'HYCU en Amérique du Sud et en Asie/Pacifique restent limitées.

IBM

IBM est l'un des Visionnaires de ce Magic Quadrant. Son portefeuille de sauvegarde principal comprend IBM Storage Defender, IBM Storage Protect, IBM Storage Protect Plus, IBM Storage Protect Snapshot et IBM Storage Protect for Cloud. Les opérations d'IBM sont géographiquement diversifiées, et ses clients ont tendance à être de grandes entreprises. Durant la période d'évaluation, IBM a publié Storage Defender, basé sur l'IA, pour l'analyse des données de plusieurs capteurs afin de détecter et de surveiller les menaces. Parmi les autres fonctionnalités notables de Storage Defender, on note l'intégration de la détection des menaces prenant en charge les applications IBM FlashSystem, les instantanés de stockage principal immuables, un plan de contrôle Defender SaaS, un modèle de licence par abonnement avec des unités de ressources flexibles et une prise en charge étendue de la virtualisation OpenShift. IBM a aussi présenté Storage Defender Data Protect, en partenariat avec Cohesity.

Points forts

- **Axé sur le stockage IBM :** les produits de sauvegarde IBM offrent des performances de sauvegarde et une résilience des données supérieures pour le stockage IBM. IBM s'est concentré sur l'amélioration de l'intégration de la sauvegarde et de récupération au stockage IBM, améliorant les performances de sauvegarde et la résilience des données.
- **Sauvegarde de conteneur OpenShift :** IBM continue d'investir de manière significative dans IBM Storage Protect Plus pour la sauvegarde et la récupération de conteneurs. Les nouveaux

produits IBM sont notamment la protection des environnements Red Hat OpenShift, Kubernetes et Tanzu.
- **Mise en œuvre de l'IA pour la détection des menaces** : IBM Storage Defender utilise un modèle d'IA développé par IBM pour l'analytics comportemental, la détection de la corruption en ligne et la détection des anomalies par application, pour la détection précoce des menaces de logiciels malveillants et des ransomware.

Réserves
- **Élargissement de la gamme de produits :** IBM a apporté des changements significatifs à son portefeuille de produits, dont l'élargissement de sa gamme de produits et de récents changements de noms de produits. Ce qui risque de générer une certaine confusion dans l'esprit des clients quant au produit le plus adapté à leurs besoins.

- **Étendue des fonctionnalités en dehors du portefeuille IBM :** l'offre Storage Defender et le message marketing d'IBM sont fortement axés sur l'intégration à son propre portefeuille de stockage. Aussi, les clients doivent vérifier au préalable la validité de ses fonctionnalités pour un stockage non IBM.

- **Dépendances de produits tiers** : les solutions Storage Defender Data Protect et Storage Protect for Cloud d'IBM dépendant de ses partenariats OEM tiers au niveau produit et plan de contrôle, l'innovation et le développement de produits échappe au contrôle d'IBM.

Microsoft

Microsoft est l'un des Acteurs de niche de 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 Manager (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 lancé Azure Backup Server (MABS) V4, la prise en charge de la sauvegarde de la base de données SAP HANA System Replication, la suppression logicielle améliorée pour Azure Backup, la sauvegarde du service Azure Kubernetes et la prise en charge de la restauration interrégionale pour PostgreSQL.

Points forts
- **Alignement avec l'adoption du cloud Microsoft Azure** : le portefeuille de sauvegarde et de récupération de Microsoft convient particulièrement aux clients passant de l'infrastructure sur site à Microsoft Azure par le biais de stratégies lift-and-shift.

- **Suppression réversible avec Azure Backup** : Microsoft propose désormais une fonctionnalité de suppression réversible, avec une logique de corbeille à durée de conservation prolongée facilitant la restauration des données de sauvegarde supprimées accidentellement, intentionnellement ou par malveillance.

- **Coffres de secours isolés** : Azure Recovery Services, pour la conservation des copies des données de sauvegarde Azure dans un coffre-fort numérique, isole les données des copies de

sauvegarde de production par abonnement et locataire Azure gérés par Microsoft, limitant ainsi l'accès des utilisateurs non autorisés aux données.

Réserves

- **Stratégie de protection des données fragmentée :** la stratégie globale de portefeuille de sauvegarde et de récupération de Microsoft n'indique aucun projet apparent d'alignement sur une stratégie de portefeuille unique ou multiple. Elle ne contient aucune indication quant à l'association, la planification, l'orchestration ou la conception de fonctionnalités de sauvegarde avec des services Microsoft comme Microsoft 365, Microsoft Entra ID, Microsoft Azure SQL, Microsoft Power Apps ou Microsoft Dynamics 365.

- **Fonctionnalités de protection PaaS Microsoft limitées :** Azure Backup ne s'intègre pas aux principaux services PaaS de Microsoft, comme Azure SQL, Azure Cosmos DB et Microsoft Entra ID.

- **Complexité de la gestion d'Azure Backup :** Azure Backup n'offre pas de fonctionnalités de déduplication natives, ce qui oblige les clients à déployer et gérer une instance de MABS/MARS. De plus, Azure Backup ne prend pas en charge les fonctionnalités courantes, comme le passage automatique de l'horloge à l'heure d'été.

Microsoft n'a pas répondu aux demandes d'informations supplémentaires ou de révision du contenu préliminaire de ce document. Par conséquent, l'analyse de Gartner est basée sur des sources tierces crédibles.

OpenText

OpenText est l'un des Acteurs de niche de ce Magic Quadrant. Son portefeuille de produits de sauvegarde d'entreprise se compose principalement de deux produits : Data Protector, pour les charges de travail sur site, et Data Protector for Cloud Workloads, pour les charges de travail cloud, couvrant les charges de travail IaaS et SaaS cloud. Les opérations de ce fournisseur sont géographiquement diversifiées, ses clients se trouvant principalement dans le segment du marché intermédiaire. Au cours de l'année passée, OpenText a amélioré la protection des données avec la prise en charge des rapports OpenText Magellan, de la détection des anomalies et d'OpenText Documentum. Il a également amélioré la sauvegarde et la restauration des fichiers clairsemés sur les systèmes Linux et l'immuabilité des données répliquées. Data Protector for Cloud Workloads offre désormais la prise en charge d'OpenShift Virtualization, de Kubernetes avec la Red Hat OpenShift Data Foundation et d'OpenNebula. Il offre également la protection des photos de contact dans Microsoft 365.

Points forts

- **Intégrations de portefeuille élargies d'OpenText :** OpenText a principalement investi dans l'intégration et la protection de ses solutions, notamment pour la protection des données OpenText Documentum et des fonctionnalités de reporting étendues à l'aide d'OpenText Magellan.

- **Options tarifaires d'OpenText :** OpenText propose plusieurs options de tarification, dont la tarification par fonctionnalités et par socket, pour une meilleure adaptation du coût total de possession aux exigences et aux charges de travail des clients.

- **Prise en charge étendue des hyperviseurs :** OpenText Data Protector s'intègre à plusieurs hyperviseurs, dont VMware VM, Microsoft Hyper-V, Proxmox VE, Oracle Linux Virtualization Manager, oVirt, Red Hat virtualization, Nutanix AHV, OpenStack, OpenNebula, Virtuozzo, Oracle VM VirtualBox, XenServer, XCP-ng, Huawei FusionCompute et Scale Computing HyperCore.

Réserves

- **Innovations limitées :** OpenText n'a que peu progressé dans plusieurs tendances actuelles de la sauvegarde et la récupération, comme la lutte contre les ransomware au-delà de la simple détection des anomalies, l'ajout d'un plan de contrôle SaaS hébergé par le fournisseur et la mise en œuvre de l'IA générative.

- **Absence d'une solution BaaS hébergée par le fournisseur :** OpenText ne dispose pas d'une solution BaaS axée sur les clients professionnels pour les charges de travail SaaS, cloud et sur site.

- **Intégrations étroites aux applications SaaS :** OpenText Data Protector for Cloud Workloads ne prend en charge que Microsoft 365. Il ne prend pas en charge d'autres applications SaaS comme Microsoft Entra ID, Salesforce, Google Workspace et Microsoft Power Apps.

Rubrik

Rubrik est l'un des Leaders de ce Magic Quadrant. Son portefeuille de produits de sauvegarde comprend Rubrik Security Cloud, incluant plusieurs offres de sauvegarde, de sécurité des données et de récupération avancée. Rubrik propose des solutions de protection des données BaaS/SaaS par application matérielle sur site et dans le cloud. Concentrée en Amérique du Nord et dans la région EMEA, la clientèle de Rubrik comprend principalement de grandes et moyennes entreprises. Durant la période d'évaluation, Rubrik a présenté de multiples fonctionnalités nouvelles ou améliorées, dont Ruby, un outil d'IA générative facilitant les tâches opérationnelles et de sécurité. Rubrik a également acquis Laminar, désormais intégré aux fonctionnalités de gestion de la sécurité des données de Rubrik. Outre ces améliorations, Rubrik offre désormais des fonctionnalités avancées de surveillance des données et de sécurité axées sur la détection des anomalies et des menaces, le chiffrement des machines virtuelles et la prise en charge de Microsoft Entra ID, Microsoft Active Directory, Amazon Simple Storage Service (Amazon S3) et Atlassian Jira.

Points forts

- **Innovation sur le marché :** Rubrik continue de proposer des produits innovants, par l'intégration de nouvelles technologies de sécurité des données issues de son acquisition de Laminar, l'élargissement de ses fonctionnalités de détection des cybermenaces et de récupération et de nouvelles offres de produits groupées.

- **Axé sur la simplicité et l'efficacité :** le plan de contrôle SaaS de Rubrik Security Cloud offre des fonctionnalités simplifiées d'administration client et des mises à jour automatisées. Ses services lui permettent de contrôler et d'orchestrer le déploiement des versions et d'apporter des correctifs au déploiement client.

- **Prix compétitifs :** les clients de Gartner notent que Rubrik mène actuellement d'âpres négociations, afin de proposer des prix compétitifs pour les renouvellements et les nouveaux déploiements nets.

Réserves

- **Disponibilité de l'assistance PaaS, SaaS et multicloud sélectionnée :** le rythme de prise en charge et de mise sur le marché de Rubrik pour les plateformes PaaS, SaaS et cloud courantes autres qu'Azure, AWS, GCP, Atlassian Jira et Microsoft 365, ainsi que ses options de plans de stockage multicloud, sont plus lents que ceux de ses concurrents.

- **Couverture géographique limitée :** en dehors de l'Amérique du Nord et de la région EMEA, Rubrik peine à fidéliser ses clients, en raison d'un manque de partenaires qualifiés en Asie/Pacifique et en Amérique du Sud.

- **Attentes financières de Rubrik :** les nouvelles attentes du marché public, suite à sa récente introduction en bourse (IPO), risquent de modifier le rythme d'innovation continue de Rubrik.

Unitrends

Unitrends, une entreprise Kaseya, est l'un des Acteurs de niche de ce Magic Quadrant. Son portefeuille de sauvegarde comprend Unitrends Backup Software, les applications matérielles Recovery Series Backup et la sauvegarde d'applications Spanning Backup for SaaS. Ses opérations sont géographiquement diversifiées, ses clients se trouvant principalement dans le segment du marché intermédiaire. Les nouveaux produits Unitrends de ces 12 derniers mois comprennent la sauvegarde directe vers le cloud pour les charges de travail à distance, distribuées et cloud, une architecture 100 % flash pour la reprise après sinistre en tant que service (DRaaS) cloud et de nouvelles applications matérielles Recovery Series Generation 10. De plus, Unitrends a amélioré ses fonctionnalités administrateur d'ajout de nouveaux terminaux protégés et de mise en œuvre de politiques de sauvegarde sans devoir se connecter à chaque application matérielle sur site.

Points forts

- **Administration unifiée :** Unitrends UniView offre l'accès administrateur unique à tous les composants de sa solution de sauvegarde et de récupération, dont la gestion des applications matérielles, la sauvegarde des points terminaux et les applications SaaS. Unitrends UniView étend également ses intégrations à d'autres offres Kaseya, comme KaseyaOne, Kaseya IT Glue et Kaseya Service Desk.

- **Intégration de Kaseya :** les licences Kaseya 365 regroupent les fonctionnalités de sauvegarde et de récupération d'Unitrends et des solutions Kaseya offrant une protection antivirus, la

gestion de la détection et de la réponse, et des fonctionnalités de restauration après attaque par ransomware.
- **DRaaS étendu avec objectifs de temps de récupération garantis (RTO)** : Unitrends a étendu les fonctionnalités de son offre DRaaS. Déployée dans les centres de données cloud d'Unitrends, celle-ci prend en charge les machines virtuelles VMware et Hyper-V sur site et peut être fournie avec des RTO contractuellement garantis.

Réserves
- **Adéquation entreprise limitée** : les initiatives de croissance et l'évolutivité limitées des applications matérielles d'Unitrends, principalement axé sur le marché des PME et fournissant ses solutions par l'intermédiaire de fournisseurs de services gérés, contribuent à le rendre moins adapté aux grands comptes d'entreprise.

- **Fonctionnalités multicloud limitées** : Unitrends Backup pour Microsoft Azure ne prend en charge que les machines virtuelles Azure, à l'exclusion des autres charges de travail d'Azure comme Azure SQL et Azure Blob Storage. L'extension à la prise en charge d'intégrations natives à d'autres fournisseurs de cloud, comme AWS et GCP, est toujours en cours.

- **Stratégie de protection SaaS limitée** : Unitrends reste à la traîne par rapport aux fournisseurs proposant la prise en charge d'autres applications SaaS, comme Microsoft Entra ID, ServiceNow et Atlassian Jira.

Unitrends n'a pas répondu aux demandes d'informations complémentaires. Par conséquent, l'analyse de Gartner est basée sur des sources tierces crédibles.

Veeam

Veeam est l'un des Leaders de ce Magic Quadrant. Son portefeuille de sauvegarde comprend Veeam Data Platform, Veeam Data Cloud, Veeam Data Cloud Vault et Veeam Kasten pour Kubernetes. Les opérations de Veeam sont géographiquement diversifiées, ses clients se trouvant généralement dans les segments du marché intermédiaire et des PME. Au cours des 12 derniers mois, Veeam a publié plusieurs mises à jour de produits, dont Veeam Data Platform v.12.1, comprenant de nouvelles fonctionnalités comme la détection des logiciels malveillants en ligne, l'analyse de contenu basée sur YARA, Veeam Threat Center, Veeam AI Assistant, la récupération instantanée de PostgreSQL et la sauvegarde du stockage d'objets. Veeam propose désormais ses propres services de sauvegarde gérés par le fournisseur, dont Veeam Data Cloud pour la protection de Microsoft 365, Microsoft Azure et Veeam Data Cloud Vault. En mars 2024, Veeam a, par ailleurs, acquis Coveware, une société de technologies et de services de réponse aux incidents de cyber-récupération.

Points forts
- **Réactivité sur le marché** : durant la période d'évaluation, Veeam a comblé ses lacunes en matière de couverture des tendances récentes du marché et des demandes des clients, avec sa solution BaaS pour Microsoft 365 et Azure hébergée par le fournisseur, ainsi qu'un service de coffre-fort cloud. Il a également étendu ses fonctionnalités de cyber-récupération à l'analyse

des logiciels malveillants, la détection des entropies en temps réel et un tableau de bord de reporting amélioré.
- **Acquisition de Coveware :** cette acquisition élargit les capacités d'assistance client de Veeam pour la réponse aux incidents, Coveware pouvant travailler avec les clients d'autres fournisseurs de sauvegarde. Coveware comprend également des technologies comme Recon pour le recueil de données pour l'analyse forensique et Unidecrypt pour le décryptage des données.

- **Format des données de sauvegarde auto-descriptif** : les solutions de sauvegarde de Veeam utilisent un fichier de données de sauvegarde auto-descriptif. Ce format permet la portabilité des données de sauvegarde entre les systèmes de stockage et d'autres déploiements Veeam. Le concept auto-descriptif élimine, de plus, la nécessité de gérer, protéger et recréer un catalogue.

Réserves
- **Approche réactive en matière d'innovation :** les offres de sauvegarde de Veeam sont souvent présentées et améliorées en réponse aux offres concurrentielles et à la demande des clients, plutôt qu'anticipant celles-ci par des fonctionnalités et des offres nouvelles, innovantes et différenciatrices sur le marché.

- **Les composants de base dépendent de l'infrastructure Windows** : les principaux composants de gestion du serveur Veeam Backup & Replication restent dépendants de l'infrastructure du serveur Windows, créant des dépendances pouvant avoir des implications en termes d'architecture, de sécurité et de coûts.

- **Protection limitée des applications SaaS :** le portefeuille de produits de Veeam laisse à désirer par rapport à d'autres fournisseurs de ce Magic Quadrant, qui ont innové avec des fonctionnalités de protection des applications SaaS autres que Microsoft 365 et Salesforce.

Veritas

Veritas est l'un des Leaders de ce Magic Quadrant. Son portefeuille de produits de sauvegarde comprend des logiciels et des applications matérielles NetBackup pour le déploiement sur site, et Veritas Alta, composé de Veritas Alta View, Veritas Alta BaaS, Veritas Alta Data Protection, Veritas Alta Recovery Vault et Veritas Alta SaaS Protection pour le déploiement dans le cloud. Les opérations de Veritas sont géographiquement diversifiées, sa clientèle étant principalement constituée de grandes ou très grandes entreprises, avec une certaine présence sur le marché intermédiaire. Ses principaux produits sortis durant la période d'évaluation sont le service d'évaluation de la cyber-résilience Veritas, de nouvelles applications matérielles NetBackup plus performantes, la prise en charge complète de Microsoft Entra ID, la prise en charge améliorée d'Oracle VLDB et de multiples améliorations de la sécurité et de la convivialité. Autre nouveauté de Veritas : Veritas Alta Copilot, pour le dépannage et les opérations assistés par l'IA.

En février 2024, Cohesity et Veritas ont annoncé leur intention de fusionner leurs activités de protection des données d'entreprise d'ici la fin de l'année civile.

Points forts

- **REDLab en interne pour la cyber-résilience :** REDLab, le laboratoire interne de Veritas, permet d'ajouter et de tester de nouvelles signatures pour détecter les cyberattaques. Les clients bénéficient ainsi de fonctionnalités de détection des cybermenaces à jour.
- **Options exhaustives de sauvegarde et de gestion :** associées aux fonctionnalités du logiciel NetBackup et ses applications matérielles évolutives horizontalement et verticalement, les offres cloud Veritas Alta offrent aux entreprises clientes un portefeuille complet de fonctionnalités de sauvegarde et de récupération et de multiples options de déploiement et de gestion dans toutes les principales régions du monde.
- **Architecture cloud native :** les services NetBackup et Veritas Alta s'exécutent dans des clusters Kubernetes fonctionnant nativement dans Azure, AWS et GCP. Dans ce concept, les services de plan de données fonctionnent indépendamment du plan de gestion, pour une architecture multicloud élastique et intrinsèquement flexible.

Réserves

- **L'expérience de mise à niveau NetBackup est incohérente :** plusieurs clients ont indiqué que les mises à niveau des logiciels et des applications matérielles NetBackup à partir d'anciennes versions ne se déroulent pas comme prévu et nécessitent une préparation et des échanges approfondis avec l'assistance technique.
- **Peu axé sur les entreprises de taille moyenne :** Veritas privilégiant sa clientèle existante de grandes entreprises, son assistance commerciale directe aux entreprises de taille moyenne reste limitée.
- **Transaction en cours avec Cohesity :** suite à la finalisation de la fusion de Cohesity avec l'activité de protection des données d'entreprise de Veritas, ses initiatives de gestion des coûts pourraient affecter la capacité de l'entreprise fusionnée à respecter les engagements de sa roadmap.

Ajout et abandon de fournisseurs

Nous évaluons et modifions nos critères d'inclusion dans les Magic Quadrants en fonction de l'évolution du marché. En raison de ces modifications, les fournisseurs présents dans un Magic Quadrant peuvent changer au fil du temps. Si un fournisseur apparaît dans un Magic Quadrant une année, mais en est absent l'année suivante, cela n'indique pas forcément un changement d'opinion de notre part concernant ce fournisseur. Cette modification peut tout simplement résulter de l'évolution du marché et donc des critères d'évaluation, ou encore d'un changement stratégique de ce fournisseur.

Sociétés ajoutées

Aucun fournisseur n'a été ajouté.

Sociétés abandonnées

Acronis a été abandonné car il ne répondait pas aux critères d'inclusion, en raison de sa priorité accordée aux MSP et aux charges de travail des périphériques périphériques/terminaux.

Critères d'inclusion et d'exclusion

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

- La solution de sauvegarde et de récupération éligible du fournisseur doit répondre à toutes les fonctionnalités « indispensables » définies dans la section Définition du marché ci-dessus.
- Le fournisseur doit proposer au moins une solution de sauvegarde et de récupération qualifiante pour l'entreprise, disponible sur le marché depuis trois années civiles au 1er avril 2024 (c'est-à-dire qu'elle doit être disponible sur le marché depuis le 1er avril 2021 au plus tard).
- 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. Ce chiffre d'affaires ne doit pas inclure celui généré par les services de mise en œuvre ou les ventes MSP.
    - Le fournisseur doit avoir généré plus de 70 millions d'USD de chiffre d'affaires récurrent annuel (ARR) au 28 février 2024, ou
    - Il doit avoir généré plus de 30 millions d'USD de chiffre d'affaires récurrent annuel déclaré au 28 février 2024, ainsi qu'un taux de croissance du chiffre d'affaires récurrent annuel de 20 % en glissement annuel (au 28 février 2023 par rapport au 28 février 2024).
- Le fournisseur doit avoir une clientèle d'au moins 1 000 clients installés sur le marché, telle que définie dans la section Définition du marché. En outre, au moins 250 de ces 1 000 clients doivent avoir déployé sa solution de sauvegarde sur un minimum de 100 serveurs physiques ou 300 serveurs virtuels dans un site de déploiement unique ou une région sur le cloud. À l'exclusion des sauvegardes de terminaux.
- Le fournisseur doit vendre et proposer une assistance active pour ses produits de sauvegarde et de récupération sous sa propre marque dans au moins trois des quatre grandes régions du monde suivantes : Amérique du Nord, EMEA, Asie/Pacifique et Amérique du Sud. Au moins 25 % de son chiffre d'affaires récurrent annuel doit provenir de l'extérieur de sa zone géographique principale.
- 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 un chiffre d'affaires dans chacune de ces trois régions.
- Sa/ses solution(s) de sauvegarde et de récupération qualifiante(es) doit(vent) être vendue(s) et commercialisée(s) essentiellement auprès des entreprises du marché intermédiaire supérieur

et des grandes entreprises. Gartner définit le marché intermédiaire supérieur comme une entreprise de 500 à 999 employés, et la grande entreprise comme une entreprise de 1 000 employés ou plus.
- Pour être pris en compte dans l'évaluation, les nouveaux produits ou les mises à jour de produits existants lancés au cours des douze (12) derniers mois doivent être disponibles au grand public depuis le 1er avril 2024 au plus tard. Tous les composants doivent être publiquement disponibles, expédiés et inclus dans la liste de prix publiée par le fournisseur à cette date. Les produits expédiés après cette date ne pourront influer que sur l'analyse de l'Exhaustivité de la vision.

- Le fournisseur doit employer au moins 100 collaborateurs à temps plein, ingénierie, vente et marketing confondus, au 28 mars 2024.

- Le produit peut être vendu soit sous forme d'offre logicielle uniquement, soit sous forme de stockage de sauvegarde intégré ou d'application virtualisée (application de sauvegarde et stockage de sauvegarde en une seule offre complète), soit sous forme d'offre de sauvegarde en tant que service basée sur SaaS, développée et hébergée par le fournisseur.

Les critères d'exclusion suivants s'appliquent :

- Vendeurs proposant des produits ou des solutions dont le logiciel provient principalement d'un fournisseur indépendant de logiciels (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. Par exemple, les applications matérielles de déduplication conçues sur mesure, SAN (storage area network), NAS (network-attached storage) ou le stockage d'objets.

- Fournisseurs qui effectuent des sauvegardes directement sur le cloud public sans stocker de copie locale sur site.

- Fournisseurs dont le chiffre d'affaires produits (plus de 75 % du chiffre d'affaires total) provient principalement de l'hébergement de centres de données et de prestataires de services gérés.

- Produits ou solutions conçus et principalement positionnés comme solutions pour environnements homogènes – comme des outils spécifiquement conçus pour la sauvegarde d'Amazon S3, Azure Blob, Amazon EC2 ou Azure Virtual Machines, ou Microsoft Hyper-V, VMware, Red Hat ou de conteneurs.

- Produits ou solutions conçus et principalement positionnés comme solutions de sauvegarde d'applications SaaS uniquement.

- Produits ou solutions conçus et principalement positionnés comme solutions de sauvegarde des terminaux, comme les ordinateurs portables, les ordinateurs de bureau et les appareils mobiles.

- Produits ou solutions conçus et principalement positionnés comme solutions de sauvegarde des bureaux distants, des sites Edge et des environnements du marché intermédiaire inférieur/PME.
- Produits ou solutions conçus et principalement positionnés pour la sauvegarde de stockage spécifique ou de vendeurs de systèmes convergents.
- Produits servant uniquement d'outils de réplication et de reprise après sinistre.
- Produits servant essentiellement à gérer les fonctionnalités d'instantané et de réplication des baies de stockage.
- Produits principalement positionnés pour la gestion des données de copie ou les tests DevOps.
- Produits principalement positionnés comme solutions de protection continue des données.

Mentions honorables

Gartner suit plus de 30 fournisseurs sur ce marché. 13 d'entre eux remplissaient les critères d'inclusion de ce Magic Quadrant. Cependant, l'exclusion d'un fournisseur ne signifie pas que le fournisseur et ses produits manquent de viabilité. Vous trouverez ci-après des fournisseurs notables qui ne répondaient pas à tous les critères d'inclusion, mais peuvent être appropriés en fonction des besoins des clients :

- **Bacula Systems** : ce fournisseur de solutions logicielles de sauvegarde et de récupération pour entreprise est basé en Suisse. Bacula Systems propose des offres logicielles open source et de produits sous licence commerciale et pris en charge. Bacula Systems a été exclu de ce Magic Quadrant, car il ne répondait pas aux critères de chiffre d'affaires.
- **Huawei Technologies** : ce fournisseur de solutions logicielles de sauvegarde et de récupération pour entreprise est basé en Chine. Huawei Technologies propose des offres basées sur des logiciels, des applications matérielles et des BaaS. Huawei a été exclu de ce Magic Quadrant car son produit éligible ne répondait pas aux critères de calendrier de disponibilité générale mondiale requis.
- **NAKIVO** : basé aux États-Unis, ce fournisseur de solutions logicielles de sauvegarde et de récupération pour l'entreprise propose des offres logicielles. NAKIVO a été exclu de ce Magic Quadrant, car il ne répondait pas aux critères de chiffre d'affaires.

Critères d'évaluation

Capacité d'exécution

Les critères de capacité d'exécution pour ce Magic Quadrant sont les suivants :

Produit ou service : ce critère couvre l'évaluation de la capacité du fournisseur à fournir des caractéristiques et fonctionnalités différenciées, prenant en charge les cas d'utilisation du

marché, les diverses utilisations par les clients de l'ensemble de son portefeuille et l'étendue des problèmes affectant l'expérience client.

Viabilité globale : ce critère couvre l'évaluation des indicateurs clés de croissance de la clientèle, du personnel et des finances du fournisseur.

Exécution commerciale / tarification : ce critère couvre l'évaluation de la réussite d'un fournisseur sur le marché. Les éléments pris en compte sont les résultats des activités nouvelles et récurrentes, le nombre de nouveaux clients de sauvegarde et de récupération et l'évolution des investissements clients. L'adaptation des efforts de vente et de prévente et le niveau de transparence tarifaire sont également pris en compte.

Réactivité sur le marché/antécédents : ce critère évalue la capacité du fournisseur à fournir des produits et des fonctionnalités qui sont les premiers sur le marché et se différencient de la concurrence, tout en continuant à répondre aux demandes du marché et à combler les lacunes de son portefeuille.

Exécution marketing : ce critère évalue la capacité du fournisseur à créer une image de marque, à s'étendre à de nouveaux marchés et à développer un pipeline de ventes sur le marché.

Expérience client : ce critère évalue la capacité du fournisseur à démontrer la satisfaction du client dans la durée et ses améliorations, et à fournir des fonctionnalités d'assistance client distinctes.

Opérations : ce critère a été exclu de cette étude en raison de la différenciation limitée des fournisseurs et des impacts en résultant sur les clients.

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

Critères d'évaluation	*Coefficient*
Produit ou service	Élevée
Viabilité globale	Moyenne
Exécution commerciale/tarification	Moyenne
Réactivité sur le marché/antécédents	Élevée
Exécution marketing	Faible

Critères d'évaluation	*Coefficient*
Expérience client	Élevée
Opérations	Non notée

Source : Gartner (août 2024)

Exhaustivité de la vision

Les critères d'exhaustivité de la vision pour ce Magic Quadrant sont les suivants :

Connaissance du marché : ce critère évalue la capacité du fournisseur à comprendre les besoins des clients, à adapter ses produits et services à ces besoins et à faire évoluer sa vision produits en fonction de ses propres convictions concernant l'orientation du marché.

Stratégie marketing : ce critère évalue la clarté de la vision marketing du fournisseur, notamment sa capacité de différenciation concurrentielle et sa connaissance des personna impliqués lors de la sélection des solutions.

Stratégie commerciale : ce critère évalue la capacité du fournisseur à établir et actualiser sa stratégie de vente en fonction des objectifs de l'entreprise et de l'intérêt du client. Les autres facteurs pris en compte sont la capacité du fournisseur à atteindre les clients directement et à étendre sa couverture par son réseau de partenaires.

Stratégie de produit : ce critère évalue la planification produits du fournisseur, en particulier le comblement des lacunes, l'engagement en matière de différenciation et l'amélioration des fonctionnalités existantes.

Modèle commercial : ce critère évalue les stratégies du fournisseur pour développer son activité sur le marché.

Stratégie verticale/sectorielle : ce critère évalue la stratégie d'orientation de l'offre de produits du fournisseur, son alignement sur les fournisseurs de technologies spécifiques au secteur et ses ressources pour répondre aux exigences spécifiques du marché vertical.

Innovation : ce critère évalue la stratégie de réinvestissement du fournisseur et ses innovations distinctives dans la conception de produits, le marketing, les ventes et les préventes, ainsi que le support client.

Stratégie géographique : ce critère évalue la stratégie du fournisseur en matière d'affectation des ressources, des compétences et de son offre de produits, afin de répondre aux besoins des quatre

grandes régions du monde : Amérique du Nord, EMEA, Asie/Pacifique et Amérique du Sud.

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

Critères d'évaluation	*Coefficient*
Connaissance du marché	Élevée
Stratégie marketing	Moyenne
Stratégie commerciale	Moyenne
Stratégie de produits	Élevée
Modèle d'entreprise	Moyenne
Stratégie verticale/sectorielle	Faible
Innovation	Élevée
Stratégie géographique	Moyenne

Source : Gartner (août 2024)

Descriptions des quadrants

Leaders

Les Leaders présentent les scores 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 les plus évolutifs, répondant aux exigences de sauvegarde et de restauration des environnements informatiques hybrides, multicloud et SaaS. Ils ont fait leurs preuves en matière de présence établie sur le marché et de performances financières. Ils sont perçus par le secteur comme des leaders d'opinion pour leur vision et des créateurs de propriété intellectuelle (PI). Ils disposent aussi de plans élaborés pour l'extension de leurs fonctionnalités générales de récupération et de cyber-récupération et de couverture des charges de travail, l'amélioration de leur facilité de

déploiement et d'administration, y compris par l'IA générative, l'augmentation de leur évolutivité et l'élargissement de leur gamme de produits. L'une des caractéristiques fondamentales des Leaders est leur capacité à adapter leur vision de la gestion de la reprise aux nouvelles exigences.

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, une caractéristique distinctive d'un Leader. Les leaders sont des fournisseurs stratégiques bien positionnés pour l'avenir, ayant réussi à répondre aux besoins des centres de données des moyennes et grandes entreprises.

Challengers

Si la capacité d'exécution des Challengers peut être satisfaisante, leur vision peut être plus limitée que celle des Leaders ou encore en phase d'élaboration ou de marketing. 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 nécessaires pour devenir potentiellement des Leaders. Pourtant, la question importante est de savoir s'ils connaissent les tendances et les exigences du marché pour réussir demain et peuvent maintenir leur dynamique en développant leur capacité d'exécution 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 ne pas avoir la capacité des Leaders à influencer les attentes des utilisateurs finaux et/ou à être envisagés pour des déploiements sensiblement plus nombreux ou importants. Les Challengers peuvent ne pas être en mesure de rivaliser de manière agressive en dehors de leur base de comptes existante et être principalement axés sur la fidélisation. Ces fournisseurs peuvent ne pas consacrer suffisamment de ressources au développement de produits attrayants pour l'ensemble du secteur et de fonctionnalités différenciées en temps opportun. Ils peuvent ne pas commercialiser efficacement leurs fonctionnalités et/ou exploiter pleinement un nombre suffisant de ressources sur le terrain pour accroître leur présence sur le marché.

Visionnaires

Les Visionnaires sont tournés vers l'avenir, développent leur portefeuille par anticipation ou sont 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 se différencient principalement par l'innovation produit et les avantages perçus par les clients. Cependant, ils n'ont pas encore créé de solution complète, ni développé leurs ventes et leur marketing à grande échelle. Ils n'ont pas encore réussi à partager leur vision, ni fait leurs preuves en matière de déploiements réussis dans de nombreuses grandes entreprises, nécessaires pour obtenir la visibilité élevée des Leaders.

Certains fournisseurs sortent du quadrant des Visionnaires pour entrer dans celui 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 celui 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 fonctionnalités relativement étendues, mais pas à très grande échelle, ni avec le succès global des concurrents d'autres quadrants. Dans certains cas, les Acteurs de niche réussissent très bien dans le segment des entreprises de taille moyenne à grande. Ils peuvent aussi saisir des opportunités de vente aux grandes entreprises, mais d'offres et de services généraux, incomplètes par rapport à ceux d'autres fournisseurs axés sur le marché des grandes entreprises.

Les Acteurs de niche peuvent se concentrer sur des zones géographiques ou des marchés verticaux spécifiques, ou un déploiement de sauvegarde ou un service de cas d'utilisation ciblé, ou simplement avoir des ambitions modestes et/ou des fonctionnalités globalement inférieures à leurs 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 de fonctionnalités complètes, ni fait preuve d'une vision ou capacité d'exécution étendue.

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 facteurs technologies, opérations et consommation appropriés pour leurs entreprises en :

- Investissant dans des solutions de sauvegarde répondant aux exigences de protection des données des environnements de centres de données, hybrides, multicloud et SaaS. Favorisant les solutions offrant une vision unifiée pour la gestion de ces environnements distribués.
- Choisissant des solutions de sauvegarde comprenant ou intégrant la protection des données de sauvegarde des attaques par ransomware, la détection des anomalies dues à des ransomware et des logiciels malveillants, ainsi que des fonctionnalités de récupération accélérée suite à une attaque par ransomware.
- Privilégiant les solutions offrant des fonctionnalités de test et d'orchestration régulière de la récupération des applications et des données.
- Développant des fonctionnalités de résilience par des solutions fournisseurs prenant en charge ou fournissant des offres de coffre-fort de données immuable et d'environnement de récupération isolé.
- Évaluant le niveau de résilience de la sauvegarde principale et la nécessité d'investir dans des sauvegardes supplémentaires, comme le cloud, la prise en charge du verrouillage d'objets, des coffres-forts de données immuables ou de la bande.

- Choisissant des produits offrant des fonctionnalités de test de récupération sécurisée et granulaire.
- Alignant leur architecture de sauvegarde sur les besoins de récupération opérationnelle de l'entreprise. Optimisant l'utilisation du stockage de sauvegarde par le stockage sur disques, comme des applications matérielles de sauvegarde dédiées ou des systèmes de fichiers distribués, le stockage d'objets ou SAN pour la récupération opérationnelle, et l'utilisation de la bande sur site, de stockage objet ou de cloud public ou hébergé par un fournisseur stockage pour la conservation à long terme et les copies sous vide d'air.
- Étudiant les implications financières à long terme des différents modèles de tarification proposés par les fournisseurs - par VM, sockets, nœuds, universel, To front-end, To back-end et agents. Investissant dans le modèle adéquat en fonction de la roadmap de l'entreprise en matière d'applications et d'infrastructure.
- Choisissant des fournisseurs prenant en charge la hiérarchisation des sauvegardes vers le cloud public et au sein de celui-ci, afin de réduire les coûts de stockage en sauvegarde. Choisissant des solutions prenant en charge la récupération d'applications à partir de sauvegardes dans le cloud public, pour les cas d'utilisation de reprise après attaque par ransomware, de test/développement ou DR.
- Sélectionnant des fournisseurs capables d'accroître la valeur des données de sauvegarde au-delà des événements de récupération. Donnant la priorité aux solutions comprenant l'analyse des données sensibles et l'e-découverte, répondant aux exigences de conformité, prenant en charge l'analytique et d'autres enrichissements de données, réutilisant les données de sauvegarde pour les tests/le développement et fournissant des fonctionnalités complémentaires comme la reprise après sinistre.

Vue d'ensemble du marché

Le marché des logiciels de sauvegarde et de récupération pour l'entreprise a connu une transformation significative au cours des deux dernières années. Les fournisseurs de sauvegarde et de récupération pour l'entreprise évalués dans ce Magic Quadrant innovent et modifient le marché dans les domaines suivants :

- **Plans de contrôle basés sur le SaaS :** de plus en plus de fournisseurs offrent des plateformes de gestion centralisées hébergées par le fournisseur de sauvegarde. Ces plateformes remplacent les déploiements gérés par le client dans sa propre infrastructure de cloud public ou de centre de données.
- **Élargir les fonctionnalités de l'IA générative :** les fournisseurs de ce marché n'ont pas tardé à présenter leurs premières offres de fonctionnalités d'IA générative. Ces solutions visent principalement à faciliter les tâches administratives de sauvegarde et le dépannage. Les mises en œuvre comprennent l'utilisation de chatbots et des dialogues de questions en langage naturel et réponses basées sur l'IA. L'utilisation de l'IA générative devrait conduire à des niveaux d'automatisation élargis pour accélérer la récupération et simplifier l'administration.

- **Protection multicloud :** alors que les entreprises 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.

- **Protection des applications et des données natives du cloud :** les fournisseurs de ce marché élargissent leur couverture de services cloud supplémentaires, afin d'augmenter la capacité de leurs clients à protéger les applications cloud natives. L'éventail des exigences exige que les fournisseurs étendent la protection à davantage d'infrastructures DBaaS, IaaS et PaaS, à plusieurs emplacements de données cloud et à la configuration d'applications cloud. Les fonctionnalités du fournisseur peuvent comprendre la découverte automatisée des applications, l'intégration aux services cloud pour orchestrer et stocker des instantanés natifs, et la réutilisation du logiciel de sauvegarde existant « en l'état » dans le cloud pour fournir une sauvegarde basée sur les agents des applications hébergées dans le cloud.

- **Détection et récupération des ransomware :** les fournisseurs ont développé des fonctionnalités de détection des attaques par ransomware en surveillant les anomalies comportementales des données protégées, et ajoutent la détection des logiciels malveillants fournie en partenariat avec des fournisseurs de sécurité ou en développant ces fonctionnalités 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 personnalisés, associant plusieurs points de récupération et en créant un environnement de test et de récupération isolé. Les fournisseurs proposent aussi désormais la récupération personnalisée d'instantanés, une fonctionnalité associant plusieurs instantanés à la dernière version de fichier scanné, propre et sûre, disponible pour restauration. Cette fonctionnalité élimine la nécessité d'effectuer plusieurs restaurations granulaires à partir de divers instantanés et restaure la mise à jour la plus récente.

- **Offres BaaS :** les principaux fournisseurs de sauvegarde étendent les fonctionnalités BaaS aux environnements sur site, IaaS, PaaS et SaaS. Les clients de Gartner investissent dans des offres BaaS complétant ces déploiements de la sauvegarde sur site, afin de simplifier la protection des environnements, y compris les charges de travail sur site sélectionnées et le cloud Edge et public.

- **Offres étendues en tant que service :** les principaux fournisseurs du marché proposent de nouveaux services complétant leur offre de sauvegarde et de récupération. Ces nouveaux services visent à étendre les services à la prise en charge de la protection et la récupération suite à une attaque par ransomware. Plusieurs fournisseurs proposent désormais des offres de stockage cloud hébergé par le fournisseur. Ces offres sont souvent appelées « coffres-forts de données immuables » (IDV) ou « coffres-forts cloud ». Les principaux fournisseurs du marché étendent ce service aux fonctionnalités de détection des anomalies et des logiciels malveillants. Certains fournisseurs proposent en outre des services d'orchestration facilitant les tests, le nettoyage et la validation de routine, ainsi que la récupération.

- **Utilisation de l'intelligence artificielle et du machine learning (ML) :** certains fournisseurs proposent des algorithmes basés sur l'IA/le ML pour les fonctionnalités de détection des anomalies dues à des ransomware et l'amélioration des pratiques en matière d'assistance client. Les nouvelles fonctionnalités comprennent des avancées dans la classification automatisée des données et les activités administratives basées sur la conversation.

- **Prise en charge des applications SaaS :** les responsables I&O commencent 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 proposent une sauvegarde Microsoft 365 et Salesforce par l'intermédiaire de partenaires ou ont développé ces fonctionnalités en interne. Les fournisseurs innovent pour protéger d'autres applications SaaS et accélérer l'intégration de nouvelles applications. Une protection supplémentaire des applications SaaS est disponible sur le marché pour les applications comme Microsoft Entra ID, Microsoft Dynamics 365, Microsoft Power Apps, Atlassian Jira et ServiceNow.

- **Récupération instantanée des bases de données, des machines virtuelles et des systèmes de fichiers :** la plupart des fournisseurs prennent en charge la récupération instantanée des machines virtuelles en installant la machine virtuelle sauvegardée directement sur l'hôte de production via le système de fichiers réseau. Les machines virtuelles deviennent ainsi instantanément disponibles, alors que le processus de récupération réel est initié en arrière-plan. Des fournisseurs comme Cohesity et Rubrik offrent la 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 Server Message Block en lecture seule.

- **Modèles de licences :** si certaines options de licences perpétuelles restent disponibles, la plupart des fournisseurs de cette recherche proposent désormais des modèles de licences par abonnement pour leurs offres logicielles. La plupart des offres de licence par abonnement sont des accords sur plusieurs années. La licence basée sur la consommation est une tendance émergente permettant d'acquérir une licence en fonction de l'utilisation mesurée à 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.

Viabilité globale : la viabilité analyse la santé financière globale de l'entreprise, le succès financier et pratique de son service commercial et la probabilité que celui-ci continue à investir dans le produit, à proposer le produit et à faire avancer la technologie du portefeuille de produits de l'entreprise.

Exécution commerciale/tarification : les capacités d'un fournisseur dans toutes les activités préliminaires à la vente et 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 gré des opportunités qui se présentent, des actions de la concurrence et de l'évolution des besoins du client et de la dynamique du marché. 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'entreprise afin d'influencer le marché, de promouvoir la marque et l'entreprise, de sensibiliser le marché aux produits proposés et de créer une image positive du produit/de la marque et de la société et l'identification avec ceux/ci dans l'esprit des acheteurs potentiels. Cette « notoriété » peut résulter de l'effet conjugué 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 notamment la façon dont les clients reçoivent l'assistance 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, d'accords de niveaux de service (SLA), etc.

Opérations : aptitude d'une entreprise 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'entreprise d'exercer son activité de façon toujours efficace et efficiente.

Exhaustivité de la vision

Connaissance 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 la plus complète sont à l'écoute des acheteurs et savent comprendre leurs désirs et leurs besoins. Ils peuvent ainsi façonner ou enrichir leurs attentes grâce à leur vision.

Stratégie marketing : série de messages clairs et différenciés, communiqués avec cohérence dans toute l'entreprise 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'entreprise 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 : l'approche du fournisseur pour le développement et la fourniture de ses produits. La stratégie doit mettre en valeur la différenciation, les fonctionnalités, la méthodologie et les caractéristiques en fonction des besoins actuels et futurs.

Modèle d'entreprise : bien-fondé et logique de l'offre commerciale de base du fournisseur.

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

Innovation : affectation 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 de ciblage de ses ressources, compétences et produits en fonction des besoins précis de régions géographiques en dehors du territoire initial, de façon directe ou par le biais de partenaires, de canaux et de filiales implantés dans ces autres territoires et marchés.

algorithmes, des logiciels ou des technologies connexes.

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.