Magic Quadrant pour les solutions logicielles de sauvegarde et de restauration d'entreprise

28 juillet 2022 - ID G00756210 - 40

Par **et 2 autres**Michael Hoeck, Nik Simpson,

La protection des environnements hybrides, SaaS et multicloud, la préparation aux attaques de ransomware et la nécessité de simplifier la sauvegarde et la gestion des données obligent les leaders de l'I&O à restructurer leur infrastructure de sauvegarde et à explorer d'autres solutions. Cette recherche fournit des analyses des fournisseurs de sauvegarde et de restauration.

Définition/description du marché

La vision de Gartner du marché des solutions logicielles de sauvegarde et de restauration d'entreprise est axée sur les technologies ou approches transformationnelles répondant aux besoins émergents des utilisateurs finaux. Il n'est pas axé sur le marché comme il l'est aujourd'hui. Selon la définition de Gartner : « Les solutions logicielles de sauvegarde et de restauration d'entreprise sont conçues pour capturer une copie instantanée (sauvegarde) des charges de travail d'entreprise dans des environnements sur site, hybrides, multicloud et SaaS et écrire les données sur une cible de stockage secondaire dans le but de récupérer ces données en cas de perte. "

Les solutions de sauvegarde et de restauration ont plusieurs fonctionnalités de base. Il s'agit notamment de la sauvegarde et de la restauration des systèmes d'exploitation, des fichiers, des bases de données et des applications dans le centre de données local ; de la sauvegarde et de la restauration des données IaaS, PaaS et SaaS du cloud public ; de la création de plusieurs copies de la sauvegarde pour prendre en charge la résilience, la reprise après sinistre et d'autres cas d'utilisation ; l'attribution de plusieurs politiques de sauvegarde et de rétention qui s'alignent sur les objectifs de récupération de l'organisation ; et le signalement des succès et des échecs des tâches de sauvegarde/restauration.

Des fonctionnalités supplémentaires peuvent être fournies par la solution. Ils protègent d'autres charges de travail, notamment les conteneurs, les sites de succursales périphériques/distantes et les terminaux; hiérarchisent les données de sauvegarde sur plusieurs cibles, y compris le cloud public; étendent les cas d'utilisation des données de sauvegarde à la découverte de données, à la conformité, à la gestion des copies de données et à la découverte électronique; à la récupération sur matériel nu; à la protection contre les ransomwares, à la détection d'anomalies de données et

de logiciels malveillants, et à la récupération avancée; et aux processus de reprise après sinistre orchestrés.

La solution peut être proposée sous forme d'appliance, de logiciel uniquement ou de sauvegarde en tant que service développée et hébergée par le fournisseur.

Quadrant magique

Figure 1 : Magic Quadrant pour les solutions logicielles de sauvegarde et de restauration d'entreprise

Source : Gartner (juillet 2022)

Points forts et mises en garde des fournisseurs

Acronis

Acronis est un visionnaire dans ce Magic Quadrant. Il est leader avec la plate-forme Acronis Cyber Protect Cloud, un service de sauvegarde et de sécurité basé sur le cloud destiné au marché intermédiaire. Le produit est fourni par plus de 20 000 fournisseurs de services via 42 centres de données Acronis répartis dans toutes les principales zones géographiques. Le fournisseur

propose également Acronis Cyber Protect, une solution logicielle qui peut être déployée sur site, fournissant une solution intégrée de sauvegarde, de sécurité et de gestion des terminaux pour les serveurs physiques, les machines virtuelles (VM) sur site, les charges de travail SaaS et les terminaux. Au cours de la période d'évaluation, Acronis a introduit de nouvelles fonctionnalités telles que les sauvegardes immuables et l'intégration avec VMware Cloud Director ; acquis 5nine, DeviceLock et Nyotron; et ouvert 12 nouveaux centres de données.

Forces

- **Fonctionnalités intégrées de cybersécurité et de protection des données —** Acronis propose un large portefeuille intégré qui combine une sécurité complète, une sauvegarde et une reprise après sinistre (DR) et une gestion informatique dans une solution unifiée unique.
- **Prise en charge de Scale Computing —** Acronis Cyber Protect prend entièrement en charge la sauvegarde/restauration sans agent pour l'hyperviseur Scale Computing HC3 afin d'étendre les capacités des cas d'utilisation en périphérie.
- **Environnements périphériques mondiaux et stratégie de protection des terminaux** — Acronis propose une solution de protection des données solide et différenciée pour les sites distants/emplacements périphériques et les points de terminaison localisés dans plus de 25 langues.

Précautions

- **Capacités limitées des entreprises et des clouds publics** : Acronis est à la traîne de la concurrence en matière de capacités d'entreprise, avec un retard dans la prise en charge des bases de données d'entreprise, des architectures de cluster, des systèmes d'exploitation, des NAS, de l'intégration du stockage et de l'intégration du cloud public.
- **Concentration limitée sur les charges de travail d'entreprise** : le portefeuille global et la stratégie d'acquisition d'Acronis sont fortement ciblés sur les fonctionnalités des terminaux, fournissant des solutions de gestion, de sécurité, de protection et de collaboration dans une solution unifiée.
- **Forte dépendance vis-à-vis des fournisseurs de services gérés (MSP) —** Acronis se concentre principalement sur la vente par l'intermédiaire de MSP pour fournir une solution gérée offrant sauvegarde, reprise après sinistre, cybersécurité, collaboration et gestion des terminaux. Les relations commerciales et l'expérience client, y compris le support, la sécurité et la performance, seront la responsabilité du MSP choisi.

Arcserve

Arcserve est un Challenger dans ce Magic Quadrant. Le portefeuille de sauvegarde d'Arcserve comprend Arcserve UDP, Arcserve Backup, Arcserve UDP Appliances, Arcserve Cloud Direct, Arcserve UDP Cloud Hybrid Secured by Sophos, Arcserve OneXafe storage appliances et Arcserve SaaS Backup. Les activités d'Arcserve sont géographiquement diversifiées et la plupart de ses clients se situent dans le segment du marché intermédiaire. Au cours de la période d'évaluation,

Arcserve a fusionné avec StorageCraft, lancé de nouvelles appliances de la série N basées sur Nutanix, étendu la capacité de l'appliance UDP à 1 Po, publié une nouvelle sauvegarde SaaS Arcserve via un accord OEM avec Keepit et publié UDP 8.1, qui inclut la prise en charge d'Oracle Standard Edition et de l'authentification multifacteur.

Forces

- **Offre d'appliances sécurisées** — Arcserve a élargi son offre d'appliances pour inclure une offre intégrée basée sur Nutanix Mine Integrated Backup qui inclut Arcserve UDP et Sophos Intercept X for Server.
- **Option de stockage immuable** — La fusion de Arcserve avec StorageCraft a élargi ses options cibles de stockage de sauvegarde avec ses offres d'appliances de stockage OneXafe. Livré avec UDP, OneXafe ajoute la possibilité de stocker des sauvegardes sur un stockage immuable.
- **Détection gratuite des logiciels malveillants Sophos** — Arcserve fournit aux clients une copie gratuite de Sophos Intercept X avec des achats éligibles de ses appliances Arcserve, de ses logiciels UDP et d'UDP Cloud Hybrid.

Précautions

- **Capacités limitées de détection et de récupération des ransomwares** — Arcserve UDP ne prend pas en charge la détection des anomalies, ce qui limite sa capacité à détecter les activités suspectes telles que le chiffrement. Arcserve UDP n'offre pas d'environnement de récupération isolé ni de conseils sur le meilleur point de récupération.
- **Prise en charge limitée des charges de travail cloud natives** — Arcserve est à la traîne des principaux acteurs en matière de prise en charge de la sauvegarde sans agent des charges de travail cloud telles qu'AWS EC2, AWS VMware Cloud, Azure VM, VMware on Azure, GCE ou VMware on GCP.
- **Absence de sauvegarde de conteneur** — Arcserve ne fournit pas de fonctionnalités de sauvegarde pour les charges de travail de conteneur.

Cohémence

Cohesity est un leader dans ce Magic Quadrant. Son portefeuille de produits de sauvegarde se compose de DataProtect et DataProtect fournis en tant que service, une offre de sauvegarde en tant que service (BaaS) qui fait partie du portefeuille de gestion des données en tant que service (DMaaS). Les activités de Cohesity sont réparties en Amérique du Nord, en Europe de l'Ouest et en Asie/Pacifique. Ses clients ont tendance à se situer dans les segments supérieurs du marché intermédiaire et des entreprises. Au cours de la période d'évaluation, Cohesity a présenté sa reprise après sinistre (DR) SiteContinuity en tant que service, des intégrations DataProtect étendues avec Oracle ZDLRA, PostgreSQL, CockroachDB, IBM Db2, SAP IQ, les instantanés VMware sur HPE Alletra, NetApp et Nutanix, Amazon C2S et Azure Stack Hub. Il a ajouté une protection continue des données pour MongoDB, Cloud Archive et Cloud Archive Direct. Le BaaS

offre une prise en charge supplémentaire des charges de travail pour les machines physiques, Hyper-V et Oracle.

Forces

- **Gestion unifiée et simplifiée** — La facilité d'administration est assurée par la gestion centralisée de plusieurs environnements Cohesity. Il s'agit notamment d'activités d'opérations BaaS autogérées et gérées par Cohesity, telles que la sauvegarde, la détection/alertes de ransomware et la reprise après sinistre. L'efficacité de la mise à l'échelle est disponible sans avoir besoin de serveurs de sauvegarde supplémentaires, de plusieurs proxys ou de matériel séparé ; et les optimisations de la déduplication, de la recherche globale et de la restauration efficace trouvent un écho auprès des clients.

- **Défense contre les menaces** — L'approche de sécurité en couches complète de Cohesity comprend des fonctionnalités intégrées ainsi que des intégrations avec des solutions de partenaires de sécurité tierces pour lutter contre les ransomwares et autres vulnérabilités.

- **Licences flexibles** — Cohesity a introduit de nouvelles licences flexibles qui permettent aux clients de déplacer des licences existantes entre une infrastructure autogérée et un BaaS géré par Cohesity.

Précautions

- **Délai demise sur le marché inflexible pour les lancements de produits** — La cadence de sortie récente des produits de Cohesity et le délai entre l'annonce et la disponibilité générale sont en retard par rapport aux années précédentes.

- **La capacité actuelle de la solution BaaS est limitée** : Cohesity BaaS ne prend pas en charge une copie localisée du jeu de données de sauvegarde, ce qui a un impact sur les performances de sauvegarde et de restauration, ainsi que sur la disponibilité en cas de panne de réseau dans le centre de données d'un client.

- **Tarification BaaS complexe** — La tarification De Cohesity pour son offre BaaS est relativement complexe, basée sur une combinaison de plusieurs critères, y compris la capacité et la rétention front-end, nécessitant des licences supplémentaires pour la capacité de consommation back-end au-delà de 30 jours.

Commvault

Commvault est un leader dans ce Magic Quadrant. Son portefeuille de sauvegarde/restauration comprend principalement Commvault Complete Data Protection, Commvault Backup & Recovery, Commvault HyperScale X et Commvault Metallic BaaS. Les activités de Commvault sont géographiquement diversifiées et ses clients ont tendance à être de grandes entreprises. Au cours de la période d'évaluation, Commvault a amélioré la gestion centralisée de ses offres Metallic et locales, de ses offres de services de récupération en direct hyper-V et de ransomware, a ajouté la prise en charge de la charge de travail cloud pour Dynamics 365, Azure Data Lake et Azure Cosmos, et a introduit un nouveau tableau de bord de sécurité Metallic et Nutanix Mine

avec Commvault. Elle a également acquis TrapX pour améliorer la détection des menaces dans son offre Metallic.

Forces

- **Prise en charge complète des charges de travail** — Commvault Complete Data Protection prend en charge un large éventail de charges de travail de manière cohérente, que ce soit dans le cloud ou sur site.
- **Options de déploiement flexibles** — Commvault propose une solution BaaS avec Commvault Metallic, une solution logicielle hybride avec Commvault Complete, une solution d'appliance évolutive avec HyperScale X et une solution de stockage basée sur le cloud géré. Tous peuvent être gérés par Commvault Command Center ou la console Web Metallic.
- **Large couverture géographique** — L'expansion de Commvault Metallic dans plusieurs zones géographiques s'aligne sur sa vaste couverture mondiale existante soutenue par les services Commvault, qui comprend un vaste écosystème de partenaires de revendeurs, d'intégrateurs et de fournisseurs de services gérés. Cela fait de Metallic un bon candidat pour les grandes entreprises ayant des participations sur les marchés matures et émergents.

Précautions

- **Complexité des opérations** — **La** stratégie de Commvault consistant à prendre en charge presque tout dans un seul produit ajoute de la complexité, ce qui fait de Commvault Complete Data Protection un choix moins adapté aux petites entreprises clientes.
- **Expérience client Variable Commvault Metallic** — Certaines demandes de Gartner mettent en évidence les défis des clients et les expériences incohérentes, principalement avec l'intégration initiale et les nouvelles charges de travail prises en charge par Commvault Metallic.
- **Sécurisé par configuration** — Commvault Les capacités complètes de sécurité et de détection des ransomwares nécessitent des services de conception et de mise en œuvre avancés pour les fournir et les activer.

Dell Technologies

Dell Technologies est un leader dans ce Magic Quadrant. Son portefeuille de logiciels de sauvegarde et de restauration se compose principalement de la suite Dell Data Protection, composée d'Avamar, NetWorker et PowerProtect Data Manager, et des services de sauvegarde APEX. Son portefeuille d'appliances comprend la série PowerProtect DP (appliances intégrées) et la série PowerProtect DD (appliances cibles). Les opérations de Dell sont géographiquement diversifiées et ses clients ont tendance à être de grandes entreprises, avec une certaine présence sur le marché intermédiaire. Au cours des 12 derniers mois, les améliorations apportées à PowerProtect Data Manager incluent des snapshots transparents pour VMware, une protection NAS dynamique et l'intégration de Cloud Snapshot Manager. Dell a également présenté apex Backup Services, PowerProtect Cyber Recovery pour Amazon AWS et Smart Scale pour les appliances powerprotect de la série DD.

Forces

- **Déploiements de coffres-forts cyber recovery —** Les clients ont accéléré le déploiement de la solution PowerProtect Cyber Recovery de Dell afin d'augmenter leurs copies de sauvegarde de production et de reprise après sinistre existantes afin d'améliorer leur posture de résilience.
- **Avancées de PowerProtect Data Manager —** PowerProtect Data Manager est désormais plus fréquemment déployé par les clients, car il inclut des fonctionnalités telles que la protection NAS dynamique, les snapshots transparents et la prise en charge de Kubernetes, qui ne sont pas disponibles dans les solutions de sauvegarde traditionnelles de Dell.
- **Relation VMware —** Dell est le premier sur le marché avec la fonctionnalité de snapshots transparents, tirant parti des nouvelles intégrations avec VMware, ce qui élimine les proxys nécessitant des proxys et atténue l'étourdissement des machines virtuelles.

Précautions

- **Nouvelles fonctionnalités limitées dans les produits Avamar et NetWorker :** Dell a réduit l'inclusion de nouvelles fonctionnalités dans ses produits Avamar et NetWorker, obligeant les clients à accélérer la mise en œuvre de Data Manager pour répondre aux nouvelles exigences.
- **Logiciels traditionnels avec appliances PowerProtect DP — Les appliances** PowerProtect DP utilisent Avamar, et Dell n'a pas encore introduit d'appliance intégrée utilisant le logiciel de sauvegarde PowerProtect Data Manager.
- **Problèmes de performances de restauration data domain —** Certains clients Gartner signalent des problèmes de performances Data Domain, en particulier pour les opérations de restauration de grande envergure à l'aide d'Avamar.

Druva

Druva est un visionnaire dans ce Magic Quadrant. La plate-forme Druva Data Resiliency Cloud est une offre BaaS qui exploite l'infrastructure AWS pour exécuter, stocker et gérer les sauvegardes. La plate-forme se compose de plusieurs produits qui fournissent une sauvegarde et une reprise après sinistre de machines virtuelles sur site et dans le cloud ; Sauvegarde et reprise après sinistre AWS natives et Kubernetes ; et la sauvegarde des applications saaS et des terminaux. Les activités de Druva sont géographiquement diversifiées, avec la plupart de ses clients en Amérique du Nord. Ses clients ont tendance à se situer dans les segments du marché intermédiaire et des entreprises. Au cours de la période d'évaluation, Druva a ajouté la prise en charge native du cloud pour AWS EC2 et AWS Kubernetes et la prise en charge de Nutanix AHV, ainsi que l'amélioration du Cloud Cache pour l'intégration de restauration instantanée VMware, la rétention à long terme et les capacités de reporting.

Forces

- **Solution BaaS SaaS mature —** Druva Data Resiliency Cloud offre une solution BaaS mature pour la protection d'une combinaison de charges de travail sur site, d'applications IaaS et cloud natives, de plusieurs charges de travail SaaS et de points de terminaison.

- **Fonctionnalités complètes de gestion des données —** Druva Data Resiliency Cloud offre des fonctionnalités complètes pour gérer la déduplication du stockage, plusieurs niveaux de stockage, la récupération par ransomware et la reprise après sinistre.

- **Licences basées sur la consommation —** Le modèle de tarification de Druva supprime les engagements à long terme et repose sur le paiement uniquement de la capacité de stockage utilisée par les clients, en tirant parti des avantages de son processus de déduplication sur plusieurs niveaux de stockage.

Précautions

- **Exigences en matière de bande passante réseau du centre de données —** La solution Druva Data Resiliency Cloud pour les charges de travail des centres de données d'entreprise — également connue sous le nom de Druva Phoenix — exige que les clients provisionnent suffisamment de bande passante réseau cloud pour prendre en charge la sauvegarde de Druva directement dans le cloud, en remplissant le cache à partir du cloud et en limitant le cache de sauvegarde local de 30 jours.

- **Limite la prise en charge du cloud natif à AWS —** Druva se concentre fortement sur la protection des charges de travail au sein d'AWS, avec des capacités natives limitées pour protéger les environnements multicloud, qui peuvent également inclure Azure et Google.

- **Emballage du produit —** Druva Data Resiliency Cloud est commercialisé et présenté comme une solution unique, mais il reste basé sur trois produits désagrégés (Phoenix pour la sauvegarde des serveurs, InSync pour les applications SaaS et la sauvegarde des terminaux, et CloudRanger pour la sauvegarde et la reprise après sinistre natives dans le cloud), ce qui se traduit par des expériences utilisateur différentes sur l'ensemble de la plate-forme.

HYCU

HYCU est un visionnaire et un nouvel entrant dans ce Magic Quadrant. HYCU Protégé est une plateforme BaaS multicloud qui s'étend sur Azure, AWS et Google pour prendre en charge les charges de travail IaaS, DBaaS, PaaS, SaaS et sur site. Les activités de HYCU sont géographiquement diversifiées, la majorité de ses clients étant en Amérique du Nord. Ses clients ont tendance à se situer dans le marché intermédiaire supérieur avec une forte concentration de clients soutenant la plate-forme Nutanix. Au cours de la période d'évaluation, HYCU a amélioré la prise en charge des sauvegardes sur site, Azure et Google, et a ajouté la prise en charge d'AWS et de Kubernetes. Il a également conclu un accord OEM pour prendre en charge les sauvegardes Microsoft 365, est passé à un modèle basé sur un abonnement et a lancé R-Score pour évaluer l'état de préparation aux ransomwares.

Forces

- **Facilité d'utilisation — Les** clients de Gartner indiquent un niveau élevé de satisfaction quant à la facilité d'utilisation, à la stabilité du produit et à 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 des centres de données avec une solution SaaS unifiée unique.
- **Intégration profonde de Nutanix —** HYCU Protégé est entièrement intégré et géré en option à partir de l'interface Nutanix Prism.

Précautions

- **Limitations sur site —** L'offre sur site de HYCU est à la traîne des principaux fournisseurs en termes de fonctionnalités telles que 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 tels qu'Oracle RAC, et la prise en charge des charges de travail non x86 telles que Power/AIX.
- **Manque d'offre d'appliances intégrées —** HYCU manque d'une offre d'appliances intégrées pour le déploiement sur site, s'appuyant sur des intégrations avec des solutions tierces telles que Nutanix Mine.
- **Capacités limitées de détection des ransomwares —** HYCU manque de détection avancée des ransomwares basée sur l'analyse des données de sauvegarde, telles que la détection du chiffrement et de l'entropie, ainsi que des capacités de guidage des points de récupération trouvées dans les offres concurrentes.

Ibm

IBM est un Challenger dans ce Magic Quadrant. Son portefeuille de sauvegarde comprend Spectrum Protect, Spectrum Protect Plus, Spectrum Protect Snapshot, Spectrum Protect Plus Online Services pour Microsoft 365 et Spectrum Copy Data Management. Les opérations d'IBM sont géographiquement diversifiées et ses clients ont tendance à être de grandes entreprises. Au cours de la dernière année, le fournisseur a publié trois mises à jour pour Spectrum Protect et Spectrum Protect Plus. Les ajouts de Spectrum Protect incluent l'authentification multifacteur, la réplication multisite, les ensembles de rétention de stockage d'objets dans le cloud et la prise en charge des niveaux de stockage cloud de Google ; et les ajouts de Spectrum Protect Plus incluent la prise en charge de Red Hat OpenShift Virtualization, la copie incrémentielle de fichiers permanents de l'instantané PVC vers vSnap et les conteneurs de sauvegarde directement sur l'objet.

Forces

- **Sauvegarde de conteneurs OpenShift —** IBM est le leader des principaux acteurs dans la prise en charge de la sauvegarde et de la restauration Red Hat OpenShift Kubernetes et IBM Cloud Paks. Les principaux avantages incluent le déploiement entièrement conteneurisé de Spectrum Protect Plus, l'intégration avec Spectrum Fusion, la prise en charge des certifications OpenShift sur Azure, IBM et Red Hat, et des intégrations CSI étendues, y compris NetApp et Hitachi.

- **Vente de portefeuille complète —** Les entreprises clientes tirent parti des solutions de sauvegarde et de restauration IBM dans le cadre d'offres packagées comprenant des systèmes IBM, du stockage, de la sécurité et des conteneurs, ce qui simplifie la gestion des fournisseurs et offre une expérience à guichet unique.

- **Stratégie produit —** Le regroupement par IBM de Spectrum Protect Suite, y compris Spectrum Protect Copy Data Management, et son introduction de Spectrum Protect Plus Online Services pour Microsoft 365 indiquent une direction de simplification et de prise en charge des charges de travail SaaS via BaaS pour le portefeuille.

Précautions

- **Gestion et architectures multiproduits —** Les cibles de stockage intégrées IBM Spectrum Protect et Spectrum Protect Plus et l'interface d'administration convergée restent en cours, ce qui nécessite l'utilisation de consoles de gestion et de cibles de stockage distinctes pour chacune.

- **Prise en charge limitée du cloud natif :** Spectrum Protect Plus ne prend pas en charge les bases de données cloud, telles qu'AWS RDS, AWS RedShift, Azure SQL Database et Google Cloud SQL, ainsi que la sauvegarde sans agent d'Azure VM, VMware on Azure, Google Compute Engine et VMware on GCP.

- **Options de services cloud limitées —** IBM est à la traîne des principaux acteurs dans l'offre de services de sauvegarde cloud gérés par les fournisseurs, tels que BaaS pour les charges de travail cloud et sur site IaaS et PaaS, ainsi que des solutions de stockage cloud de sauvegarde.

Micro Focus

Micro Focus est un acteur de niche dans ce Magic Quadrant. Son portefeuille de produits de sauvegarde se compose de deux produits distincts : Data Protector pour les charges de travail sur site et Data Protector 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 ont tendance à être principalement dans le segment du marché intermédiaire. Au cours de l'année écoulée, Micro Focus a amélioré Data Protector en améliorant les performances de sauvegarde VMware et l'intégration SAP HANA, en étendant l'échelle de déduplication logicielle à 1 Po et en introduisant Data Protector for Cloud Workloads, qui prend en charge une variété d'environnements virtuels, de systèmes IaaS cloud et de Microsoft 365.

Forces

- **Prix de l'abonnement —** Le prix par socket déjà bas de Micro Focus et les modèles de licence perpétuelle basés sur TB sont désormais complétés par des modèles de licence basés sur l'abonnement.

- **Lancement de l'offre BaaS —** Micro Focus a introduit Data Protector for Cloud Workloads par le biais d'un accord OEM. Cette offre fournit aux clients Micro Focus ses capacités cloud initiales pour protéger les charges de travail Microsoft 365 et AWS EC2 et Kubernetes.

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

Précautions

- **Manque d'intégration —** Couvrir une gamme complète de charges de travail de centre de données et de cloud nécessite des produits distincts de Micro Focus, qui manquent d'intégration significative.
- **Aucune fonctionnalité de détection de ransomware —** Micro Focus manque de capacités intégrées pour détecter les anomalies de ransomware ou les logiciels malveillants.
- **Options logicielles uniquement :** Micro Focus est à la traîne des principaux acteurs qui fournissent plusieurs stratégies et architectures de déploiement, notamment des appliances de sauvegarde intégrées, un plan de contrôle SaaS et des services de stockage en nuage gérés par le fournisseur.

Rubrik

Rubrik est un leader dans ce Magic Quadrant. Son portefeuille de produits de sauvegarde se compose principalement de Rubrik Security Cloud et de multiples offres pour l'observabilité des données et la restauration 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 ajouté l'authentification multifacteur, la prise en charge de NetApp SnapMirror, la hiérarchisation cloud supplémentaire pour Azure et AWS, la sauvegarde directe sur AWS S3 et Azure Object Store, la chasse aux menaces et l'intégration améliorée avec Nutanix AHV. Il a également introduit Rubrik Cloud Vault, la sauvegarde en tant que service Microsoft 365 et la garantie de récupération des ransomwares.

Forces

- **Facilité de déploiement et d'utilisation —** Les demandes de Gartner indiquent une satisfaction continue des clients en ce qui concerne la facilité de déploiement, la configuration et l'administration des stratégies de Rubrik, les processus de mise à l'échelle simplifiés, la recherche et l'index globaux et l'intégration des déploiements via une console de gestion centralisée.
- **Fonctions de protection et de récupération contre les ransomwares —** Rubrik propose une offre de produits complète et sécurisée qui protège le système de sauvegarde et les données contre les cyberattaques, détecte les anomalies et les logiciels malveillants dans les données de sauvegarde et fournit des fonctionnalités de récupération efficaces.
- **Adoption par les entreprises — Les** capacités de mise à l'échelle et le support client de Rubrik conduisent à un plus grand nombre de clients dans les grandes entreprises sur des marchés matures, remplaçant une variété de solutions concurrentielles différentes.

Précautions

- **Impacts sur les prix — Le** programme de matériel evergreen de Rubrik, qui fournissait du matériel d'actualisation au renouvellement, n'est plus disponible pour les nouveaux clients. Les clients existants recevront désormais des crédits logiciels pour les offres SaaS de Rubrik, ce qui nécessite une évaluation des options de licence pour éviter tout impact sur le coût total de possession.
- **Sauvegarde SaaS limitée —** Rubrik est à la traîne dans la prise en charge des applications SaaS au-delà de Microsoft 365, manquant de prise en charge de solutions telles que Salesforce, Google Workspace, Slack et MS Dynamics.
- **Intégration étroite de NAS Cloud Direct —** L'intégration de la technologie Igneous acquise reste un travail en cours, manquant d'intégration avec les capacités d'enquête sur les ransomwares et de découverte de données sensibles de Rubrik, limitant des fonctionnalités telles que la détection d'anomalies et l'identification de données sensibles.

Unitrends

Unitrends est un acteur de niche dans ce Magic Quadrant. Son portefeuille de sauvegarde comprend le logiciel de sauvegarde Unitrends, l'appliance de sauvegarde Recovery Series et spanning backup pour la sauvegarde d'applications SaaS. Les opérations du fournisseur sont géographiquement diversifiées et ses clients ont tendance à se situer dans le segment du marché intermédiaire. Au cours des 12 derniers mois, Unitrends a publié 10 mises à jour logicielles de la version 10.5.3 à la version 10.6.2. Les nouveaux produits incluent Recovery Assurance et des réplicas au niveau de l'image, ainsi que de nouveaux agents pour Oracle 19C et Red Hat 8. Les améliorations continues apportées à la plate-forme de gestion centrale UniView incluent le déploiement automatisé d'agents, les sauvegardes Google unifiées et l'authentification unique KaseyaOne.

Forces

- **Administration unifiée —** Unitrends fournit UniView, offrant un accès administratif unique à tous les composants de la solution, y compris la gestion des appliances, la sauvegarde des terminaux et les applications SaaS.
- **Portefeuille d'appliances —** Unitrends continue d'élargir son offre d'appliances avec l'ajout d'appliances de bureau des séries ION et ION+ pour les bureaux de périphérie et les petits bureaux.
- **Intégration de Kaseya —** Unitrends continue de s'intégrer plus complètement au portefeuille IT Complete de Kaseya. Cela permettra de rationaliser l'accès aux ressources techniques, de facturation et de support, et de fournir plus de fonctionnalités à ses clients.

Précautions

- **Accent sur les PME et les entreprises de taille moyenne — Les** initiatives de croissance d'Unitrend axées sur les marchés des PME et des moyennes entreprises et son évolutivité

limitée des appliances contribuent à réduire l'adéquation aux grands comptes d'entreprise.

- **Stratégie BaaS limitée —** Unitrends est à la traîne par rapport à d'autres acteurs majeurs dont les solutions BaaS gérées par les fournisseurs prennent en charge plusieurs charges de travail cloud et sur site.
- **Manque de prise en charge des conteneurs —** Unitrends n'a introduit aucune fonctionnalité pour protéger les charges de travail des conteneurs.

Veeam

Veeam est leader dans ce Magic Quadrant. Elle est en tête avec Veeam Platform, qui est composé de Veeam Backup & Replication et Veeam ONE pour la surveillance et l'analyse des sauvegardes. La sauvegarde pour les environnements de cloud public et l'orchestration de la reprise après sinistre sont activées via des modules autonomes. Les activités de Veeam sont géographiquement diversifiées et ses clients ont tendance à se situer dans les segments des entreprises et des marchés intermédiaires. Au cours des 12 derniers mois, il a publié 30 mises à jour de produits ainsi que des plug-ins pour huit partenaires OEM. Veeam a introduit des licences universelles pour remplacer les licences basées sur socket, intégré Kasten à son référentiel de sauvegarde Veeam 11 et ajouté la prise en charge d'AWS S3 Glacier et de S3 Glacier Deep Archive.

Forces

- **Quelle que soit la taille, où que vous soyez** : la conception unique des produits Veeam prend en charge les clients de toutes tailles utilisant la même base de code, qu'il s'agisse d'un particulier ou d'une grande entreprise. Il dispose d'une vaste géographie et de relations avec des partenaires pour soutenir les clients de toutes tailles et de tous emplacements.
- **Prise en charge des conteneurs Kubernetes —** Veeam a acquis Kasten en octobre 2020 et a intégré ses fonctionnalités dans son référentiel de sauvegarde évolutif Veeam de base pour fournir une prise en charge robuste des charges de travail basées sur des conteneurs.
- **Prise en charge des charges de travail et des plates-formes —** Veeam Platform s'intègre à un large éventail de plates-formes, de serveurs, de systèmes de stockage et d'applications, ainsi qu'à tous les principaux fournisseurs de services de cloud public pour prendre en charge les cas d'utilisation des centres de données, du cloud et de la périphérie.

Précautions

- **BaaS/DRaaS/stockage s'appuie sur des partenaires —** Veeam ne dispose pas d'une offre BaaS, DRaaS ou de stockage native pour ses clients. Ces services dépendent entièrement du réseau de partenaires Veeam Cloud & Service Provider (VCSP), qui peut être incohérent dans les offres et l'expérience client, et reporte le support et la responsabilité au VCSP.
- **Complexité globale : les** demandes des clients gartner indiquent que Veeam peut devenir plus complexe à gérer à mesure que la taille de l'environnement de sauvegarde augmente. Cela

inclut le déploiement d'agents Veeam distincts par environnement protégé, la gestion de plusieurs proxys de sauvegarde et la sélection appropriée de l'infrastructure de calcul et de stockage pour s'aligner sur les exigences de performance et de stockage.

- **Sécurisation par exigence de mise en œuvre** — La mise en œuvre d'une plate-forme sécurisée associée à une immuabilité, une détection et une récupération avancées des ransomwares nécessite que les clients conçoivent, déploient et gèrent soigneusement le déploiement pour atténuer les menaces de ransomware.

Veritas Technologies

Veritas Technologies est un leader dans ce Magic Quadrant. Son portefeuille de produits de sauvegarde se compose principalement de NetBackup, NetBackup Appliances et Backup Exec. Les opérations de Veritas sont géographiquement diversifiées. Ses clients ont tendance à être de grandes entreprises et il a une certaine présence sur le marché intermédiaire. Veritas a annoncé deux mises à jour majeures de NetBackup : 9.1 et 10.0. Ces mises à jour incluent des ajouts pour la sauvegarde Kubernetes, l'analyse informatique intégrée, la détection des anomalies et l'analyse des logiciels malveillants basées sur l'IA, les sauvegardes CDP, la prise en charge immuable du verrouillage des objets et l'architecture de mise à l'échelle automatique pour AWS et Azure. Veritas a également annoncé de nouvelles offres de NetBackup SaaS Protection, Access Appliance pour la conservation des données à long terme et le stockage de données basé sur le cloud NetBackup/Recovery Vault.

Forces

- **Plusieurs options de déploiement** — NetBackup offre aux clients plusieurs options de déploiement, notamment des appliances évolutives et évolutives, apportez votre propre stockage et des appliances virtualisées et conteneurisées.

- **Architecture cloud native — L'architecture** mise à jour de NetBackup fournit désormais des services de client cloud et de snapshot à mise à l'échelle automatique pour faire évoluer dynamiquement les ressources cloud selon les besoins afin de réduire l'infrastructure cloud dédiée.

- **Grande entreprise et multigéographie :** l'accent mis par Veritas sur les grandes entreprises dans plusieurs zones géographiques est soutenu par des investissements considérables dans les équipes de vente et d'avant-vente et un écosystème de partenaires bien établi pour améliorer l'expérience client.

Précautions

- **Fonctionnalités du produit liées aux licences d'abonnement** : les clients Veritas doivent passer à de nouvelles licences d'abonnement pour accéder aux nouvelles fonctionnalités basées sur le cloud ajoutées à leur offre de produits.

- **Transition de la protection SaaS** — Les clients qui utilisent Veritas SaaS Backup, un accord OEM avec Keepit, doivent transférer le support vers Keepit ou conclure un nouveau contrat de

licence avec Veritas et recommencer avec de nouvelles tâches de sauvegarde dans sa nouvelle offre NetBackup SaaS Protection.

- **Défis liés au support technique —** Certains clients de Gartner ont exprimé leur frustration face à la qualité et à la rapidité des réponses du support client.

Zerto

Zerto est un acteur de niche dans ce Magic Quadrant. La plate-forme Zerto est une solution convergente de sauvegarde et de reprise après sinistre visant à protéger les charges de travail sur site et dans le cloud. Les activités de Zerto sont géographiquement diversifiées. Ses clients ont tendance à être de grandes entreprises, et il a une certaine présence sur le marché intermédiaire. Au cours de la période d'évaluation, il a annoncé Zerto 9.0, Zerto pour Kubernetes, Zerto In-Cloud pour AWS et Zerto Backup pour SaaS. Zerto 9.0 incluait la restauration instantanée de vm à partir du journal CDP, le stockage compatible S3, la hiérarchisation des données pour AWS et Azure, l'immuabilité pour AWS S3 et la restauration et le téléchargement de fichiers en libre-service. La prise en charge de Kubernetes inclut AKS, GKE, IKS, EKS, VMware Tanzu et OpenShift. Backup for SaaS prend en charge Microsoft 365, Google Workspace, Salesforce, Active Directory et Dynamics 365.

Forces

- **Vente de solutions HPE —** Acquise par HPE en septembre 2021, Zerto est désormais en mesure d'étendre sa visibilité sur plusieurs régions et d'étendre son alignement directement avec les clients HPE.

- **Capacités CDP — Les** solutions de Zerto trouvent un écho auprès des clients qui ont besoin de capacités de protection continue des données et de reprise après sinistre prenant en charge des objectifs de point de récupération quasi nuls et granulaires des machines virtuelles dans des environnements sur site, hybrides et multicloud.

- **Prise en charge de Kubernetes —** Zerto a étendu ses solutions de protection continue des données et de reprise après sinistre à Kubernetes en utilisant sa technologie de journalisation pour restaurer les applications protégées en points de récupération granulaires.

Précautions

- **Remplacement de sauvegarde incomplet —** Zerto compte un nombre limité de clients qui utilisent son offre pour les besoins traditionnels de sauvegarde instantanée. Il continue d'être principalement déployé pour les utilisations CDP et DR.

- **Manquant de prise en charge des charges de travail non virtuelles**, la solution de Zerto se concentre spécifiquement sur les charges de travail virtuelles, excluant ses offres de la protection du stockage rattaché au réseau et des serveurs physiques.

- **Tout n'est pas CDP :** la dernière offre de Zerto pour la gestion de la reprise après sinistre AWS dans toutes les régions s'intègre à l'aide d'instantanés et d'API EBS natifs du cloud plutôt que

d’une version remaniée du CDP sur site de Zerto.

Fournisseurs ajoutés et supprimés

Nous révisons et ajustons nos critères d’inclusion pour les Magic Quadrants à mesure que les marchés changent. À la suite de ces ajustements, la composition des fournisseurs dans n’importe quel Magic Quadrant peut changer au fil du temps. L’apparition d’un fournisseur dans un Magic Quadrant une année et non la suivante n’indique pas nécessairement que nous avons changé d’opinion à l’égard de ce fournisseur. Cela peut être le reflet d’un changement dans le marché et, par conséquent, de critères d’évaluation modifiés, ou d’un changement d’orientation de la part de ce fournisseur.

Supplémentaire

HYCU

Tomber

Aucun

Critères d’inclusion et d’exclusion

Les critères suivants représentent les attributs spécifiques qui, selon les analystes, sont nécessaires pour être inclus dans cette recherche :

- Le fournisseur doit répondre à au moins un des critères de revenus suivants. Les revenus doivent provenir uniquement de son portefeuille de produits de sauvegarde et de restauration. Ces revenus ne doivent pas inclure les revenus générés par les services de mise en œuvre, l’hébergeur BaaS ou les services gérés.

- Le fournisseur doit avoir généré des revenus de licence (perpétuels et/ou d’abonnement) et de maintenance (PCGR) supérieurs à 50 millions de dollars au cours des quatre derniers trimestres se terminant le 28 février 2022 ; *(ou)* Le fournisseur doit avoir généré des licences (perpétuelles et/ou abonnements) et des revenus de maintenance (PCGR) supérieurs à 25 millions de dollars, combinés à un taux de croissance de 20 % d’une année à l’autre, au cours des quatre derniers trimestres se terminant le 28 février 2022.

- La ou les solutions de sauvegarde et de restauration éligibles du fournisseur doivent être vendues et commercialisées principalement auprès des moyennes et grandes entreprises haut de gamme. Gartner définit le marché intermédiaire haut de gamme comme étant de 500 à 999 employés, et la grande entreprise comme étant de 1 000 employés ou plus.

- Le fournisseur doit employer au moins 100 employés à temps plein dans les fonctions d’ingénierie, de vente et de marketing combinées.

- La solution de sauvegarde et de restauration éligible du fournisseur doit se concentrer sur la protection des environnements d’entreprise s’exécutant dans le centre de données (centre de données traditionnel ou installation de colocation) et protéger les charges de travail IaaS, PaaS

et SaaS basées sur le cloud. La protection des sites distants est considérée comme une extension de ces fonctionnalités de base.

- Le fournisseur doit disposer d'au moins une solution de sauvegarde et de restauration éligible disponible dans le commerce pour une utilisation par les entreprises pendant trois années civiles avant le 1er mars 2022 ; c'est-à-dire qu'il doit avoir été disponible dans le commerce au moins dès le 1er mars 2019.
- Les nouveaux produits ou les mises à jour de produits existants qui ont été lancés au cours des 12 derniers mois doivent être généralement disponibles au plus tard le 31 mars 2022 pour être pris en compte aux fins d'évaluation. Tousles produits et mises à jour doivent être accessibles au public, expédiés et inclus dans laliste de prix publiée par le fournisseur à partir de cette date. Les produits expédiés après cette date n'auront qu'une influence sur l'axe Exhaustivité de la vision.
- Le fournisseur doit servir une base installée d'au moins 1 000 clients sur le marché tel que défini dans ce Magic Quadrant. 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 seul site de déploiement ou région cloud. Cela exclut les sauvegardes de point de terminaison.
- Le fournisseur doit activement vendre et prendre en charge ses produits de sauvegarde et de restauration sous sa propre marque dans au moins trois des principales zones géographiques suivantes : Amérique du Nord, EMEA, Asie/Pacifique et Amérique du Sud. Au moins 25 % des revenus totaux doivent provenir de l'extérieur de sa principale zone géographique.
- 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 amenés à chiffre d'affaires dans chacune des trois zones géographiques.
- La solution fournisseur doit prendre en charge la sauvegarde et les restaurations granulaires des données dans chacun des environnements suivants :
  - Hyperviseur : VMware et Hyper-V via l'intégration avec les frameworks de sauvegarde fournis par ces hyperviseurs.
  - Applications : Microsoft Exchange et Microsoft SharePoint ou prise en charge de la sauvegarde Microsoft 365.
  - Systèmes d'exploitation: Windows, Linux.
  - Bases de données : sauvegarde cohérente des bases de données d'Oracle et de Microsoft SQL Server.

- Le produit peut être vendu en tant qu'offre logicielle uniquement, en tant qu'appliance de stockage de sauvegarde intégrée (application de sauvegarde plus stockage de sauvegarde dans une seule offre intégrée) ou en tant qu'offre de sauvegarde en tant que service (BaaS).

Les critères d'exclusion suivants s'appliquent :

- Fournisseurs proposant des produits ou des solutions dont les logiciels proviennent entièrement d'un fournisseur de logiciels indépendant (ISV) tiers.
- Les produits qui servent uniquement de cible ou de destination pour la sauvegarde, mais qui n'exécutent pas réellement la fonction de gestion de la sauvegarde et de la restauration. Les exemples incluent les appliances de déduplication spécialement conçues, le SAN, le NAS ou le stockage d'objets.
- Fournisseurs qui sauvegardent directement dans le cloud public sans stocker de copie locale sur site.
- Les fournisseurs dont la principale source de revenus produits (plus de 75 % du chiffre d'affaires total) provient des hébergeurs de centres de données et des fournisseurs de services gérés.
- Produits ou solutions conçus et positionnés comme des solutions de sauvegarde de terminaux tels que des ordinateurs portables, des ordinateurs de bureau et des appareils mobiles.
- Produits ou solutions conçus et positionnés comme des solutions pour sauvegarder les bureaux distants, les emplacements périphériques et les environnements de milieu de gamme/PME inférieurs.
- Produits ou solutions conçus pour des environnements homogènes, tels que des outils conçus pour sauvegarder uniquement Microsoft Hyper-V, VMware, Red Hat ou des conteneurs.
- Produits ou solutions conçus pour sauvegarder des fournisseurs de stockage ou de systèmes hyperconvergés spécifiques.
- Produits qui servent uniquement d'outils de réplication et de reprise après sinistre.
- Produits qui servent principalement à gérer les snapshots et les capacités de réplication des baies de stockage.
- Produits positionnés principalement pour la gestion des données de copie.
- Des produits qui sont principalement des solutions de protection continue des données.

Mentions honorables

Gartner suit plus de 30 fournisseurs sur ce marché. Quatorze d'entre eux répondaient aux critères d'inclusion de ce Magic Quadrant ; toutefois, l'exclusion d'un fournisseur ne signifie pas que le

vendeur et ses produits manquent de viabilité. Vous trouverez ci-dessous des fournisseurs remarquables qui ne répondaient pas à tous les critères d'inclusion, mais qui pourraient convenir aux clients, sous réserve des exigences.

Bacula Systems: Ce fournisseur de solutions logicielles de sauvegarde et de restauration d'entreprise a son siège en Suisse. Bacula Systems fournit des offres logicielles en tant qu'OpenSource et en tant que produits sous licence commerciale et pris en charge. Les solutions de Bacula Systems prennent en charge une variété de charges de travail dans les centres de données, le cloud et les cas d'utilisation en périphérie.

NAKIVO : Ce fournisseur de solutions logicielles de sauvegarde et de restauration d'entreprise a son siège social à Sparks, Nevada, États-Unis. NAKIVO fournit des solutions logicielles qui prennent en charge une variété de charges de travail dans les centres de données, le cloud et les cas d'utilisation en périphérie.

Critères d'évaluation

Capacité d'exécution

Tableau 1 : Capacité d'exécuter les critères d'évaluation

Critères d'évaluation	*Pondération*
Produit ou service	Haut
Viabilité globale	Haut
Exécution des ventes/Tarification	Haut
Réactivité au marché/Record	Haut
Exécution du marketing	Bas
Expérience client	Haut
Opérations	Non évalué

Source : Gartner (juillet 2022)

Exhaustivité de la vision

Tableau 2 : Exhaustivité des critères d'évaluation de la vision

Critères d'évaluation	*Pondération*
Compréhension du marché	Haut
Stratégie marketing	Douleur moyenne
Stratégie de vente	Douleur moyenne
Stratégie d'offre (produit)	Haut
Modèle d'affaires	Douleur moyenne
Stratégie verticale/industrielle	Douleur moyenne
Innovation	Haut
Stratégie géographique	Douleur moyenne

Source : Gartner (juillet 2022)

Descriptions des quadrants

Dirigeants

Les leaders ont les mesures combinées les plus élevées de la capacité d'exécution et de l'exhaustivité de la vision. Ils disposent des portefeuilles de produits les plus complets et les plus évolutifs. Ils ont fait leurs preuves en matière de présence établie sur le marché et de performance financière. Pour la vision, ils sont perçus dans l'industrie comme des leaders d'opinion et des créateurs de propriété intellectuelle (PI), et ont des plans bien articulés pour améliorer les capacités de récupération, améliorer la facilité de déploiement et d'administration,

et augmenter leur évolutivité et l'étendue de leurs produits. Pour que les fournisseurs connaissent un succès à long terme, ils doivent viser à prendre en charge les exigences de protection des données de l'informatique hybride. Une pierre angulaire pour les leaders est la capacité d'articuler la façon dont les nouvelles exigences seront abordées dans le cadre de leur vision de la gestion du rétablissement.

En tant que groupe, on peut s'attendre à ce que les leaders soient considérés comme faisant partie de la plupart des nouvelles propositions d'achat et qu'ils aient des taux de réussite élevés pour gagner de nouvelles affaires. Cela ne signifie toutefois pas qu'une part de marché importante constitue à elle seule un indicateur primaire 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

Les challengers peuvent exécuter aujourd'hui, mais peuvent avoir une vision plus limitée que les leaders, ou n'ont pas encore pleinement produit ou commercialisé leur vision. Ils ont des produits performants et peuvent bien fonctionner pour de nombreuses entreprises. Ces fournisseurs ont les ressources financières et commerciales et les capacités nécessaires pour potentiellement devenir des leaders. Pourtant, la question importante est de savoir s'ils comprennent les tendances du marché et les exigences du marché pour réussir demain, et s'ils peuvent maintenir leur élan en s'exécutant à un niveau élevé au fil du temps.

Un Challenger peut disposer d'un portefeuille de sauvegarde robuste, mais n'a pas encore été en mesure de tirer pleinement parti de ses opportunités ou n'a pas la même capacité que les leaders à influencer les attentes des utilisateurs finaux et/ou à être considéré pour des déploiements beaucoup plus nombreux ou plus larges. Les challengers ne peuvent pas rivaliser de manière agressive en dehors de leur base de compte existante et se concentrer principalement sur la rétention. Ces fournisseurs peuvent ne pas consacrer suffisamment de ressources de développement à la fourniture de produits présentant un large attrait pour l'industrie et des caractéristiques différenciées en temps opportun, ou peuvent ne pas commercialiser efficacement leurs capacités et / ou exploiter pleinement suffisamment de ressources sur le terrain pour se traduire par une plus grande présence sur le marché.

Visionnaires

Les visionnaires sont avant-gardistes, faisant progresser les capacités de leur portefeuille en avance, ou bien en avance, sur le marché, mais leur exécution globale ne les a pas propulsés en tant que challengers ou peut-être leaders. Souvent, cela est dû à des ventes et à un marketing limités, ou à un temps allongé pour l'installation et la configuration initiales, mais cela est parfois dû à l'évolutivité ou à l'étendue des fonctionnalités et / ou de la prise en charge de la plate-forme. Ces fournisseurs se différencient principalement par l'innovation produit et les avantages perçus pour les clients. Cependant, comme certains sont relativement nouveaux sur le marché, ils n'ont pas encore atteint l'exhaustivité de la solution ou maintenu des ventes à grande échelle, et le succès du marketing et du partage de l'esprit, ni démontré les déploiements continus et réussis des 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 parce que 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 justifie de passer aux quadrants Challengers ou Leaders, ou même de rester dans le quadrant Visionaries.

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

Les acteurs de niche peuvent se concentrer sur des zones géographiques spécifiques, des marchés verticaux ou un déploiement de sauvegarde ciblé ou un service de cas d'utilisation; ou ils peuvent simplement avoir des horizons modestes et / ou des capacités globales inférieures à celles de leurs concurrents. D'autres acteurs de niche sont trop nouveaux sur le marché ou ont pris du retard et, bien qu'ils valent la peine d'être surveillés, n'ont pas encore pleinement développé de fonctionnalités complètes ou démontré de manière cohérente une vision expansive ou la capacité d'exécution.

Contexte

Les responsables de l'infrastructure et des opérations (I&O) chargés des opérations de sauvegarde doivent repenser l'infrastructure de sauvegarde pour 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, de cloud public et de périphérie. Privilégiez les solutions qui offrent une seule vitre pour gérer ces environnements distribués.
- Choisissez des solutions de sauvegarde qui fournissent une solution complète pour la détection des anomalies et des logiciels malveillants, ainsi que des capacités de récupération accélérées contre les attaques de ransomware.
- Comprenez bien le niveau de résilience fourni sur la copie de sauvegarde principale et la nécessité d'investir dans des copies de sauvegarde supplémentaires pour garantir la résilience de la sauvegarde.
- Choisissez des produits qui offrent une expérience de test de récupération sécurisée et granulaire.
- Alignez l'architecture de sauvegarde sur les besoins de restauration opérationnelle de leur organisation. Optimisez l'utilisation du stockage de sauvegarde en utilisant des appliances de

sauvegarde sur disque ou un stockage SAN pour la restauration opérationnelle, et soit un stockage sur bande ou sur site, soit un stockage dans le cloud public pour une rétention à long terme.

- Comprendre en détail le coût total de possession 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 sortie de l'abonnement avant la fin de la période.
- Comprendre les implications à long terme sur les coûts des différents modèles de tarification proposés par les fournisseurs : basés sur les machines virtuelles, les sockets, les nœuds, les universels, les TB frontaux, les TB back-end et les agents. Investissez dans le bon modèle basé sur la feuille de route de l'application et de l'infrastructure de l'organisation.
- Sélectionnez les fournisseurs qui prennent en charge la hiérarchisation des copies de sauvegarde dans le cloud public et dans le cloud public pour économiser sur les coûts de stockage sur site. Choisissez des solutions qui prennent en charge la récupération d'applications à partir de copies de sauvegarde dans le cloud public pour répondre aux cas d'utilisation de test/développement ou de reprise après sinistre.
- Sélectionnez des fournisseurs capables d'augmenter la valeur des données de sauvegarde en les rendant disponibles pour répondre aux exigences de conformité, prendre en charge les analyses, réutiliser les données de sauvegarde pour les tests/développement et fournir des fonctionnalités complémentaires telles que la reprise après sinistre.

Aperçu du marché

Le marché des logiciels de sauvegarde et de restauration d'entreprise a subi une transformation importante au cours des deux dernières années. Les fournisseurs de sauvegarde évalués dans ce Magic Quadrant se sont principalement concentrés sur les domaines suivants :

- **Gestion centralisée : à** mesure que les entreprises s'orientent vers un modèle informatique hybride et que les charges de travail sont réparties dans le centre de données, le cloud public et la périphérie, il est essentiel de protéger ces charges de travail, quel que soit leur emplacement. Les principaux fournisseurs de sauvegarde s'attaquent à ce problème en proposant une plate-forme de gestion qui peut être déployée soit dans le centre de données principal, soit de plus en plus en tant que service hébergé dans le cloud public.
- **Résilience, détection et correction des** ransomwares : L'augmentation du nombre d'attaques de ransomware a conduit les fournisseurs à prendre des mesures concrètes pour fournir une détection et une correction des ransomwares ainsi qu'une infrastructure de sauvegarde résiliente. Alors que la plupart des fournisseurs prennent en charge la création de secondes copies immuables de sauvegarde via le stockage compatible write once, read many (WORM), d'autres fournisseurs visent à rendre le référentiel de sauvegarde principal plus résilient en prenant en charge les snapshots immuables. Les principaux fournisseurs ont mis en place des

capacités pour détecter les attaques de 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 des ransomwares en créant un environnement de test isolé et à fournir une copie de sauvegarde propre pour récupérer des fichiers spécifiques. Ces efforts restent en grande partie en cours.

- **Offres BaaS :** les principaux fournisseurs de solutions de sauvegarde étendent leurs capacités BaaS pour inclure des 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 certaines charges de travail sur site et le cloud public et périphérique.

- **Prise en charge de la sauvegarde IaaS et PaaS dans le cloud public :** au cours de la période d'évaluation, les principaux fournisseurs de sauvegarde sur site ont augmenté leurs investissements dans la création de capacités de protection des charges de travail natives du cloud, en particulier les machines virtuelles et les applications hébergées dans AWS, Microsoft Azure et Google Cloud Platform. Certains fournisseurs de sauvegarde prennent également en charge la sauvegarde de produits DBaaS tels qu'Amazon RDS, Amazon Aurora et Microsoft Azure SQL. Alors que certains fournisseurs ont intégré le logiciel de sauvegarde aux fonctionnalités de snapshot natif offertes par ces fournisseurs de cloud, la plupart continuent de réutiliser leur logiciel de sauvegarde existant « tel quel » dans le cloud pour fournir une sauvegarde basée sur un agent des applications hébergées dans le cloud.

- **Prise en charge des applications SaaS :** les leaders de l'I&O ont commencé à inclure des applications SaaS telles que Microsoft 365, Google G Suite et Salesforce dans leur stratégie de sauvegarde. La plupart des fournisseurs évalués dans cette étude ont commencé à fournir une sauvegarde Microsoft 365 via des partenaires ou à développer ces fonctionnalités en interne. La protection d'autres applications SaaS, telles que Salesforce, Microsoft Dynamics 365, ServiceNow et Workday, reste en grande partie un travail en cours.

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

- **Restauration 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 de calcul dans le cloud public. Cela permet une récupération opérationnelle rapide si l'environnement local n'est pas disponible. Les données de sauvegarde peuvent également être utilisées à des fins de test/développement dans le cloud public.

- **Sauvegarde de base de données NoSQL** : alors que les entreprises traditionnelles continuent d'exécuter leurs applications métier de base sur des bases de données de système de gestion de base de données relationnelle (RDMS) telles qu'Oracle et Microsoft SQL, les projets de mode 2 tels que le Big Data exploitent généralement des bases de données NoSQL telles que MongoDB et Cassandra. Au fur et à mesure que ces projets commencent à prendre de l'ampleur et à apporter une valeur tangible, il est de plus en plus nécessaire de protéger ces environnements. Des fournisseurs établis tels que Commvault, Dell Technologies et Veritas Technologies ont commencé à répondre à ces exigences de sauvegarde en intégrant ces fonctionnalités de manière native dans la plate-forme de sauvegarde. Des fournisseurs tels que Rubrik et Cohesity ont fait des acquisitions stratégiques dans ce domaine.

- **Restauration instantanée des bases de données, des machines virtuelles et des systèmes de fichiers** : la majorité des fournisseurs prennent en charge la récupération instantanée des machines virtuelles en montant la machine virtuelle sauvegardée directement sur l'hôte de production via NFS. Les machines virtuelles peuvent ainsi devenir instantanément disponibles, tandis que le processus de récupération réel peut être lancé en arrière-plan. Des fournisseurs tels que Cohesity et Rubrik offrent une restauration instantanée de bases de données telles que Microsoft SQL et Oracle, tandis que Veeam offre également un accès instantané au partage de fichiers à partir de sauvegardes via un partage de fichiers SMB en lecture seule.

- **Sauvegarde de conteneurs** : les principaux fournisseurs ont annoncé la prise en charge de la sauvegarde de conteneurs, soit en intégrant ces fonctionnalités de manière native dans leur plate-forme existante, soit par le biais d'acquisitions. Bien que les demandes des clients Gartner montrent un faible intérêt pour la sauvegarde des conteneurs, nous prévoyons qu'elle augmentera en adoption, car davantage de conteneurs utilisant un stockage persistant sont déployés pour prendre en charge les charges de travail de production.

- **Modèlesde licences perpétuelles** : Bien que certaines options de licence perpétuelle restent disponibles, tous les principaux fournisseurs de ce marché sont passés à la fourniture de leurs offres logicielles par le biais de modèles de licence par abonnement. La plupart des offres de licence par abonnement sont des contrats à durée de plusieurs années. Les licences basées sur la consommation sont une tendance émergente pour les licences qui offrent la possibilité de concéder des licences sur ce qui est utilisé en fonction de la mesure à des intervalles plus fréquents.

Définitions des critères d'évaluation

Capacité d'exécution

Produit/Service : Biens et services de base offerts par le fournisseur pour le marché défini. Cela inclut les capacités actuelles des produits / services, la qualité, les ensembles de fonctionnalités, les compétences, etc., qu'ils soient offerts nativement ou par le biais d'accords / partenariats OEM tels que définis dans la définition du marché et détaillés dans les sous-critères.

Viabilité globale : La viabilité comprend une évaluation de la santé financière globale de l'organisation, du succès financier et pratique de l'unité d'affaires et de la probabilité que l'unité d'affaires individuelle continue d'investir dans le produit, continue d'offrir le produit et fasse progresser l'état de l'art au sein du portefeuille de produits de l'organisation.

Exécution des ventes/tarification : les capacités du fournisseur dans toutes les activités d'avant-vente et la structure qui les prend en charge. Cela inclut la gestion des transactions, la tarification et la négociation, le support avant-vente et l'efficacité globale du canal de vente.

Réactivité au marché / Record: Capacité de réagir, de changer d'orientation, d'être flexible et d'atteindre le succès concurrentiel à mesure que les opportunités se développent, que les concurrents agissent, que les besoins des clients évoluent et que la dynamique du marché change. Ce critère tient également compte de l'historique de réactivité du fournisseur.

Exécution du 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, d'accroître la notoriété des produits et d'établir une identification positive avec le produit / la marque et l'organisation dans l'esprit des acheteurs. Ce « partage d'esprit » peut être motivé par une combinaison de publicité, d'initiatives promotionnelles, de leadership éclairé, de bouche à oreille et d'activités de vente.

Expérience client : Relations, produits et services/programmes qui permettent aux clients de réussir avec les produits évalués. Plus précisément, cela inclut la façon dont les clients reçoivent un support technique ou un support de compte. Cela peut également inclure des outils auxiliaires, des programmes de support client (et leur qualité), la disponibilité de groupes d'utilisateurs, des accords de niveau de service, etc.

Opérations : La capacité de l'organisation à atteindre ses objectifs et ses engagements. Les facteurs comprennent la qualité de la structure organisationnelle, y compris les compétences, les expériences, les programmes, les systèmes et autres véhicules qui permettent à l'organisation de fonctionner de manière efficace et efficiente sur une base continue.

Exhaustivité de la vision

Compréhension du marché : Capacité du vendeur à comprendre les désirs et les besoins des acheteurs et à les traduire en produits et services. Les fournisseurs qui montrent le plus haut degré de vision écoutent et comprennent les désirs et les besoins des acheteurs, et peuvent façonner ou améliorer ceux-ci avec leur vision supplémentaire.

Stratégie de marketing : Un ensemble clair et différencié de messages communiqués de manière cohérente dans toute l'organisation et externalisés par le biais du site Web, de la publicité, des programmes clients et des énoncés de positionnement.

Stratégie de vente: La stratégie de vente de produits qui utilise le réseau approprié d'affiliés de vente directe et indirecte, de marketing, de service et de communication qui étendent la portée et la profondeur de la portée du marché, des compétences, de l'expertise, des technologies, des services et de la clientèle.

Stratégie d'offre (produit) : Approche du fournisseur en matière de développement et de livraison de produits qui met l'accent sur la différenciation, les fonctionnalités, la méthodologie et les ensembles de fonctionnalités lorsqu'ils correspondent aux exigences actuelles et futures.

Modèle d'affaires : La solidité et la logique de la proposition commerciale sous-jacente du fournisseur.

Stratégie verticale/sectorielle : Stratégie du fournisseur visant à orienter les ressources, les compétences et les offres pour répondre aux besoins spécifiques de segments de marché individuels, y compris les marchés verticaux.

Innovation : Agencement direct, connexe, complémentaire et synergique des ressources, de l'expertise ou du capital à des fins d'investissement, de consolidation, défensives ou préventives.

Stratégie géographique : Stratégie du fournisseur visant à orienter les ressources, les compétences et les offres pour répondre aux besoins spécifiques des zones géographiques en dehors de la géographie « d'origine » ou de la géographie native, soit directement, soit par l'intermédiaire de partenaires, de canaux et de filiales, selon les besoins de cette géographie et de ce marché.

quant à l'exactitude, l'exhaustivité ou la pertinence de ces informations. Bien que les recherches de Gartner puissent aborder des questions juridiques et financières, Gartner ne fournit pas de conseils juridiques ou d'investissement et ses recherches ne doivent pas être interprétées ou utilisées comme telles. Votre accès et votre utilisation de cette publication sont régis par la politique d'utilisation de Gartner. Gartner est fier de sa réputation d'indépendance et d'objectivité. Sa recherche est produite indépendamment par son organisme de recherche sans apport ni influence d'un tiers. Pour de plus amples renseignements, voir « Principes directeurs sur l'indépendance et l'objectivité ».