Magic Quadrant pour les plateformes de sauvegarde et de protection des données

24 juin 2025 - ID G00824107 - 47 minutes de lecture

De : Michael Hoeck, Jason Donham, René Rodriguez, Rizvan Hussain, Sankalp Rastogi

Les fournisseurs de plateformes de sauvegarde et de protection des données améliorent continuellement leurs offres de sauvegarde pour renforcer la protection des données des entreprises dans les environnements multicloud, SaaS et de centre de données. Cette étude vise à permettre aux responsables I&O d'identifier et de sélectionner les fournisseurs répondant à leurs besoins en matière de protection des données d'entreprise.

Hypothèses de planification stratégique

- D'ici à 2029, 75 % des entreprises utiliseront une solution commune de sauvegarde et de récupération des données hébergées sur site et dans l'infrastructure cloud, contre 25 % en 2025.

- D'ici à 2029, 80 % des entreprises considéreront la sauvegarde des applications SaaS comme une exigence majeure, contre 20 % en 2025.
- D'ici à 2029, 95 % des plateformes de sauvegarde et de protection des données comprendront une technologie intégrée de détection et d'identification des cybermenaces, contre 55 % en 2025.
- D'ici à 2029, 85 % des grandes entreprises adoptent la sauvegarde en tant que service (BaaS), parallèlement aux déploiements gérés par le client et à la sauvegarde des charges de travail cloud et sur site, contre 25 % en 2025.
- D'ici à 2029, 90 % des plateformes de sauvegarde et de protection des données intègreront l'IA générative pour améliorer leurs opérations de gestion et de support, contre moins de 25 % en 2025.
- D'ici à 2029, 35 % des entreprises mettront en œuvre des capacités d'IA agentique pour l'automatisation des opérations de sauvegarde, contre moins de 2 % en 2025.
- D'ici à 2029, 30 % des entreprises intégreront les copies de sauvegarde comme source de données pour l'analytics et l'inférence, contre moins de 5 % en 2025.

Définition/description du marché

Gartner définit les plateformes de sauvegarde et de protection des données comme des technologies permettant de capturer des copies ponctuelles des données d'entreprise, afin de pouvoir les restaurer dans des scénarios multiples de perte de données, de renforcer les stratégies de protection des données, et d'étendre les insights de données et les capacités d'accès. Ces

technologies protègent les données, les applications et l'infrastructure de l'entreprise dans les environnements hybrides, multicloud et SaaS. Les plateformes de sauvegarde et de protection des données sont disponibles sous forme de logiciels uniquement, d'appliances logicielles intégrées et de BaaS (sauvegarde en tant que service) développées et hébergées par le fournisseur.

La protection et la récupération des données d'applications d'une entreprise, quel que soit le type d'infrastructure sous-jacente et son emplacement, sont plus importantes que jamais. Alors que l'environnement des entreprises devient de plus en plus complexe, les solutions de plateforme de sauvegarde et de protection des données protègent leurs données, qu'elles résident dans des environnements 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, dû à une défaillance matérielle ou logicielle, à des erreurs opérationnelles, à des attaques malveillantes ou à des incidents d'environnement, les entreprises utilisent ces solutions pour récupérer et restaurer en toute fiabilité 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 des environnements de plus en plus complexes et divers. Cela comprend des capacités de test, d'accélération et d'orchestration des réponses de récupération de données après sinistre physique ou lié à un cyber-événement.

De plus, allant au-delà des cas d'utilisation de récupération traditionnels, ces solutions augmentent la valeur générée par les données copiées sur la

plateforme pour l'entreprise. Elles intègrent les cas d'utilisation axés sur l'activation par les données, comme le renforcement de la protection des données et des intégrations d'infrastructure, et l'extension des insights et de l'accès aux données.

Ces capacités de protection renforcées comprennent la découverte des applications, des fonctionnalités avancées de préparation à la cyberreprise, l'orchestration des tests et processus de reprise après sinistre ou cyberattaque, la découverte des données et le suivi de l'accès. Ces intégrations s'étendent aux échanges bidirectionnels d'insights opérationnels avec d'autres plateformes d'infrastructure et d'exploitation, comme celles dédiées au réseau, au stockage et à la sécurité.

Les solutions des fournisseurs permettent l'accès aux données par d'autres profils utilisateurs que les administrateurs de la sauvegarde, grâce aux insights de données et aux capacités d'accès. Ces nouveaux profils utilisateurs comprennent de nouveaux profils IT comme la sécurité, les DevOps, les données et l'analytics, ainsi que d'autres utilisateurs métiers comme la conformité et le service juridique.

Caractéristiques essentielles

- Sauvegarde des données et des systèmes dans des environnements hybrides, multicloud et SaaS :
  - L'hybride prend en charge l'infrastructure sur site et cloud public. Les exigences hybrides comprennent la protection des systèmes d'exploitation, des hyperviseurs, des fichiers, des bases de données, des machines virtuelles et des applications.
  - Les exigences multicloud et SaaS comprennent la protection de l'infrastructure en tant que service (IaaS) dans au moins deux

environnements de prestataires de services de cloud public et au moins deux applications SaaS majeures, comme Microsoft 365, Salesforce et Google Workspace.

- 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 policies 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.

- Des capacités de préparation à la cyberreprise, comme la détection des anomalies et de l'entropie après sauvegarde, développées par le fournisseur ou tierces intégrées.

- Une console centralisée pour la gestion de l'infrastructure de solutions de sauvegarde distribuées dans les environnements hybrides et multicloud.

Caractéristiques communes

- Protection cloud native ou sans agent des données critiques intégrée dans les applications de type plateforme en tant que service (PaaS) proposées par des prestataires de services cloud, comme Amazon Relational Database Service (RDS), Google Bigtable ou Microsoft Azure SQL

- Protection des données critiques dans les applications SaaS, comme Atlassian Jira, Microsoft Entra ID, ServiceNow, Slack et Workday

- 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)
- Capacités de découverte d'applications sur site et dans le cloud permettant d'identifier les composants d'application, les dépendances et l'état de protection des données et d'effectuer la sauvegarde et la récupération de l'application
- Plan de contrôle SaaS hébergé par le fournisseur pour la gestion et l'orchestration des environnements complexes et distribués
- Offre BaaS hébergée par le fournisseur : services de sauvegarde et de récupération pour les environnements hybrides et multicloud
- Fonctionnalités d'IA générative simplifiant l'administration, améliorant les services d'assistance et accélérant les procédures de sauvegarde et de récupération
- Fonctionnalités de sécurité avancées, comme l'authentification multifacteur, les contrôles d'accès basés sur les rôles, la validation des modifications multipersonnes, l'intégration de solutions de gestion des accès privilégiés, 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
- Application des principes de vérification systématique (zero-trust) dans les pratiques de conception, d'architecture et de déploiement de solutions, garantissant le plus haut niveau de sécurité et d'intégrité des données

- Fonctionnalités avancées de préparation à la cyber-récupération, comme la détection intégrée d'anomalies et d'entropie en temps réel développée par le fournisseur ou par un tiers, détection de logiciels malveillants et basée sur des signatures, après sauvegarde ou à la demande, et solutions de coffre-fort de données immuables et d'environnement de reprise isolé
- Orchestration des tests et processus de reprise après sinistre et de cyber-récupération
- Prise en charge de cas d'utilisation de plateforme étendue pour la protection des données, la conformité, la gestion des données de copie et les exigences de test et de développement
- Prise en charge de fonctionnalités élargies d'analyse et d'accès aux insights de données de sauvegarde, comme la catégorisation et la classification des données, la détection de données sensibles, la recherche, les investigations, l'analyse décisionnelle (business intelligence), la génération augmentée par la récupération (RAG) et d'autres formes de récupération via API
- Contrôles d'accès basés sur les rôles fournissant l'accès aux données de sauvegarde à d'autres profils utilisateurs outre les équipes d'administration de la sauvegarde, comme les services sécurité, juridique, conformité et les équipes en charge des données et de l'analytics

Magic Quadrant

Figure 1: Magic Quadrant for Backup and Data Protection Platforms

Points forts et points faibles des fournisseurs

Arcserve

Arcserve est l'un des Acteurs de niche de ce Magic Quadrant. Le portefeuille de sauvegarde et de protection des données d'Arcserve comprend Arcserve Unified Data Protection (UDP), Arcserve Backup, les applications matérielles Arcserve série 10000, Arcserve UDP Cloud Hybrid 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. Durant la période d'évaluation, Arcserve a lancé les versions UDP 10 et 10.1, avec l'ajout d'Assured Security pour les tests de reprise après sinistre, la mise en attente virtuelle à la demande vers le cloud et la réplication simultanée. Il a également actualisé ses offres d'appliances matérielles avec son appliance 10K qui propose des améliorations du RTO et du RPO, la détection des logiciels malveillants, le chiffrement en ligne et des tests automatisés de reprise après sinistre. Arcserve a également lancé Arcserve Cloud Storage, son offre de stockage cloud géré, et Arcserve Cyber Resilient Storage, sa cible de stockage définie par logiciel pour la sauvegarde.

Points forts

- **Options de tarification souples :** Arcserve propose à ses clients le choix entre des licences perpétuelles et des abonnements à durée déterminée, avec plusieurs statistiques disponibles, dont le volume de téraoctets en front-end et le nombre de sockets et de machines virtuelles, afin de répondre à un large éventail de besoins des acheteurs en matière de modèles tarifaires.

- **Renouvellement de l'investissement produit :** durant cette étude, Arcserve a amélioré sa cadence de lancement de nouveaux produits et fonctionnalités, dont une version actualisée de son logiciel UDP, une série d'appliances UDP rénovée et une plateforme de test de reprise après sinistre.

- **Stockage immuable défini par logiciel :** Arcserve a lancé Cyber Resilient Storage, une cible de stockage de sauvegarde définie par logiciel pour son offre UDP, offrant le choix entre des options de stockage sur site et dans le cloud. Cette solution offre des capacités de stockage immuables intégrées pouvant être déployées en tant qu'ISO pour une installation

bare-metal, en tant que machine virtuelle ou dans un cloud géré par Arcserve.

Réserves

- **Prise en compte limitée des grandes entreprises :** Arcserve étant axé sur le marché des entreprises de taille moyenne et la distribution croissante de ses solutions par des prestataires de services gérés, ses initiatives de croissance et sa stratégie produit risquent de limiter sa pertinence pour les comptes de grandes entreprises.

- **Sauvegarde dans le cloud peu développée :** au-delà de la protection des applications SaaS, le portefeuille de produits d'Arcserve offre une prise en charge multicloud et des intégrations cloud natives limitées, et nécessite le recours à des agents. Ses offres de logiciels, de stockage de sauvegarde défini par logiciel et d'appliances ciblent essentiellement les usages sur site et proposent des intégrations de stockage cloud en tant que cible de sauvegarde.

- **Absence d'IA :** le portefeuille actuel et la roadmap produit à court terme d'Arcserve ne prévoient 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 pour l'administration et le support.

Cohesity

Cohesity est l'un des Leaders de ce Magic Quadrant. Ses portefeuilles de sauvegarde DataProtect et NetBackup sont disponibles pour un déploiement géré par le client, sur site et dans le cloud ou comme offre en tant que service. Les opérations de Cohesity sont géographiquement diversifiées. Ses clients vont des segments du marché intermédiaire supérieur aux très

grandes entreprises. Durant la période d'évaluation, Cohesity a présenté NetBackup 11, offrant des fonctionnalités comme le chiffrement post-quantique, la certification Sheltered Harbor, la chasse aux menaces basée sur des fonctions de hachage et la surveillance des risques liés aux modifications suspectes de policies et de connexions. De plus, l'entreprise a amélioré l'orchestration de la récupération NetBackup avec des répétitions programmées, une récupération intercloud/régionale et des recommandations de points de récupération automatisés. Elle a amélioré sa solution DataProtect par l'ajout de sauvegardes cloud immuables, la détection renforcée des menaces et la prise en charge de Couchbase NoSQL via un agent connecteur et Cohesity Gaia, avec de nouvelles sources de données et types de fichiers, un visualiseur de sujets, et des temps de réponse plus rapides. Cohesity a également mis à jour DataProtect as a Service avec la prise en charge de Microsoft Entra ID, la récupération des groupes Microsoft 365, l'intégration du stockage de sauvegarde Microsoft 365 et l'ajout d'une option de déploiement autonome pour sa plateforme de contrôle Helios.

In En décembre 2024, Cohesity a finalisé sa transaction, intégrant le portefeuille de protection des données d'entreprise de Veritas à ses propres activités. Cohesity offre désormais les gammes de produits NetBackup et Alta Data Protection.

Points forts

- **Gamme complète de produits :** avec l'acquisition de NetBackup et d'Alta Data Protection de Veritas, Cohesity élargit son expertise technique et ses capacités produit à la prise en charge des écosystèmes d'entreprise complexes, tout en offrant une couverture exhaustive de la charge de travail pour les systèmes sur site, multicloud et SaaS.

- **Large couverture géographique :** le rachat du portefeuille de protection des données Veritas, de son infrastructure mondiale étendue et de ses équipes de support permet à Cohesity d'atteindre désormais les marchés mondiaux sur lesquels Veritas avait une présence établie.

- **Services améliorés de réponse aux cyberincidents :** l'équipe CERT (Cyber Event Response Team) de Cohesity propose des services de réponse aux incidents (IR) pour la gestion de la réaction et de la récupération durant un cyber-événement. L'équipe CERT offre des capacités de réponse aux incidents renforcées, en association avec des fournisseurs tiers leaders du secteur, comme Mandiant et Palo Alto Networks.

Réserves

- **Redondance des produits après la fusion :** le rachat de NetBackup par Cohesity pourrait susciter des limitations de ressources pour les gammes de produits communes, ralentissant potentiellement le rythme de développement de produits sur l'ensemble du portefeuille. Le portefeuille regroupant les offres de NetBackup/Alta Data Protection et de Cohesity se traduit par une redondance des produits et capacités.

- **Manque de cohérence dans la tarification et les remises :** certains clients ont exprimé des réserves concernant les pratiques tarifaires et de remises de Cohesity – les solutions Cohesity pouvant sembler plus coûteuses que celles des concurrents directs lors des négociations initiales.

- **Récupération limitée de l'infrastructure d'application cloud :** Cohesity dispose de capacités limitées en matière de récupération complète des applications/de l'infrastructure, notamment pour la prise en charge des déploiements d'infrastructure-as-code (IaC) et des configurations cloud,

ce qui complique la récupération des applications dans les scénarios de reprise à grande échelle.

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. Durant la période d'évaluation, Commvault a lancé la prise en charge de la récupération au niveau de la forêt Microsoft Active Directory, Cloud Rewind, Clumio Backtrack, amélioré ses opérations de cyberrésilience Cleanroom Recovery et ajouté l'assistance pour le stockage Amazon Web Services (AWS) à son offre Air Gap Protect. Commvault a également amélioré Commvault Cloud Threat Scan et Command Center pour Oracle et SAP HANA et ajouté de nouvelles intégrations bidirectionnelles avec CrowdStrike Falcon Insight XDR et Splunk SOAR. En avril 2024, Commvault a racheté Appranix, puis Clumio en octobre 2024. Ces rachats étendent respectivement la récupération des infrastructures d'applications cloud de Commvault et la prise en charge d'AWS.

Points forts

- **Couverture complète de la charge de travail sur le cloud :** la couverture de Commvault en matière de cloud IaaS et PaaS est étendue, avec la prise en charge native d'Oracle et de Microsoft Azure DevOps, ainsi que la couverture cloud gouvernementale pour AWS, Azure et Oracle Cloud Infrastructure (OCI).

- **La stratégie Cloud Rewind :** le rachat d'Appranix par Commvault offre des capacités améliorées pour la découverte, la protection et la récupération

de l'infrastructure des applications cloud, dont une protection orchestrée complète de la pile d'applications et des vitesses de récupération accélérées.

- **Récupération orchestrée d'Active Directory :** la récupération orchestrée d'Active Directory au niveau de la forêt par Commvault est conforme aux bonnes pratiques de Microsoft et accélère la récupération d'Active Directory. La récupération au niveau de la forêt est intégrée aux capacités de récupération granulaire de sauvegarde d'Active Directory et d'Entra ID de Microsoft.

Réserves

- **Complexité de la configuration initiale :** certains clients de Gartner évoquent des difficultés liées aux principes de conception initiaux du produit lors du choix entre une architecture gérée par le client et BaaS, et des difficultés à trouver une documentation adéquate pour l'auto-résolution des problèmes de configurations.

- **Expérience de retard du support client :** des clients ont fait part de critiques concernant leur expérience avec l'équipe de support Commvault, les experts métiers (SME) au-delà du support de premier niveau n'étant pas facilement accessibles.

- **Absence d'une console de gestion unifiée :** nécessitant deux outils d'administration différents pour la gestion intégrale, la transition du Commvault Command Center à la parité de fonctions avec la console Java n'est pas encore achevée. La documentation fait référence aux deux méthodes de gestion, plutôt que de diriger les utilisateurs exclusivement vers la console Web.

Dell Technologies

Dell Technologies est l'un des Leaders de ce Magic Quadrant. Son portefeuille de logiciels de sauvegarde et de protection des données comprend PowerProtect Data Manager, PowerProtect Cyber Recovery, CyberSense, NetWorker, PowerProtect Backup Services et les appliances PowerProtect. Les opérations de Dell sont géographiquement diversifiées et ses clients principalement de grandes entreprises du marché intermédiaire. Durant la période d'évaluation, les améliorations notables apportées à PowerProtect Data Manager sont l'ajout de la protection directe du stockage pour PowerMax et PowerStore, la détection d'anomalies des machines virtuelles et des systèmes de fichiers, et la protection de la virtualisation Red Hat OpenShift. Dell a également lancé de nouvelles appliances Data Domain, dont une architecture de référence 100 % flash, et de nouveaux packages PowerProtect Backup Services regroupant Microsoft 365, Google Workspace et la protection des terminaux sous une seule licence, avec Salesforce Data Archiver comme offre produit autonome.

Points forts

- **Protection du stockage Dell :** PowerProtect Data Manager s'intègre aux baies de stockage Dell PowerStore et PowerMax, par Storage Direct Protection et DD Boost. Cela offre une protection efficace des données pour les charges de travail importantes, répondant en particulier aux besoins des applications sensibles à la performance.

- **Intégration d'AI Factory de Dell :** l'offre AI Factory de Dell pour l'infrastructure d'IA sur site comprend l'intégration à PowerProtect Data Manager. Cette intégration protège ses métadonnées Kubernetes, ses modèles de données d'entraînement, ses bases de données vectorielles et ses configurations et paramètres.

- **Amélioration de la détection et de la réponse gérées :** Dell a lancé un service de détection et de réponse gérées incluant une licence pour la

plateforme CrowdStrike Falcon XDR, l'intégration renforcée à PowerProtect Data Manager et les journaux d'activité PowerProtect Data Domain. Ce service de Dell analyse les indicateurs de compromission (IOC) et alerte les clients en fonction de l'activité détectée.

Réserves

- **Retard en termes de fonctions différenciatrices sur le marché :** par rapport à d'autres fournisseurs leaders du marché, Dell accuse un certain retard en matière de découverte et de récupération complètes des applications cloud, ainsi que d'extension des données de sauvegarde à des cas d'utilisation supplémentaires, comme la détection de données sensibles, la RAG et d'autres méthodes de récupération des données via API.
- **Administration de solutions complexes :** certains clients de Dell trouvent son administration multi-produit trop complexe pour l'orchestration et la gestion du déploiement de sa solutoin de sauvegarde et de protection des données.
- **Exigence de cyberdétection multi-produit :** Dell PowerProtect Data Manager offre la détection des anomalies basée sur les métadonnées, nécessitant la mise en œuvre des solutions Dell PowerProtect Cyber Recovery et CyberSense pour effectuer l'inspection complète de l'intégrité des fichiers, l'analyse avec des règles YARA et la recherche de logiciels malveillants.

Druva

Druva est l'un des Leaders de ce Magic Quadrant. Druva Data Security Cloud est son offre principale de sauvegarde et de protection des données. Les opérations de Druva sont géographiquement diversifiées, la majeure partie

de ses clients se trouvant dans les segments entreprises et marché intermédiaire. Durant la période d'évaluation, Druva a ajouté la sauvegarde inter-cloud avec Azure Storage, l'intégration à Microsoft Sentinel et Microsoft Security Copilot et des services de détection et de réponse gérés des données (MDDR). Druva a également lancé l'outil Dru Investigate alimenté par l'IA, accélérant l'analyse et la réponse aux menaces, et la détection d'anomalies par IA pour Microsoft 365 et VMware, et Druva Microsoft 365 Backup Express, utilisant le stockage de sauvegarde Microsoft 365.

Points forts

- **Fiabilité de l'exécution de la stratégie produit :** s'appuyant sur son architecture de plateforme SaaS améliorée hébergée sur AWS, Druva a accéléré la livraison de nouvelles offres et intégrations critiques. Celles-ci comprennent l'introduction d'une option de locataire de stockage Azure Cloud pour la sauvegarde des machines virtuelles AWS EC2 et Azure, la prise en charge de Microsoft Entra ID et Microsoft Dynamics 365, et la sauvegarde sans agent pour Microsoft Azure SQL. Ce fournisseur a, de plus, ajouté des capacités de protection optimisées pour Amazon S3, Amazon RDS et le stockage en réseau (NAS).

- **Assistance opérationnelle et insights de sécurité optimisés par l'IA :** Dru Assist améliore l'expérience utilisateur grâce à des rapports interactifs, des workflows guidés et un dépannage intelligent. Il comprend Dru Investigate pour la sécurité, permettant de détecter les menaces internes, d'analyser les anomalies et d'accélérer la réponse aux incidents.

- **Défense proactive contre les ransomware :** Druva propose un service géré gratuit en tant que capacité native comprise dans sa plateforme de protection des données, offrant une cyberrésilience proactive pour les sauvegardes des clients. Ce service permet la surveillance, la détection

avancée des menaces et la réponse aux incidents 24 h/24, 7 j/7, selon des playbooks personnalisés axés sur la neutralisation précoce des menaces et garantissant une récupération fiable des données.

Réserves

- **Dépendance envers AWS :** basée sur l'infrastructure AWS, la couche de gestion et d'orchestration de la plateforme Druva peut susciter des difficultés pour les entreprises privilégiant d'autres fournisseurs cloud ou des policies d'évitement du multi-cloud.
- **Prise en charge limitée de Google Cloud Platform (GCP) :** la protection de Google Cloud Compute Engine repose sur des méthodes basées sur des agents, et la prise en charge native des services PaaS de GCP est en retard par rapport aux principaux fournisseurs de cloud, nécessitant une évaluation attentive des besoins spécifiques de protection des charges de travail GCP.
- **Prise en charge limitée de MongoDB et Cassandra :** sauvegarde native prenant en compte les applications pour les bases de données MongoDB et Apache Cassandra fait défaut à Druva. Les entreprises qui les utilisent devront s'appuyer sur d'autres outils tiers ou les fonctionnalités de sauvegarde natives, ce qui complique les opérations ou entraîne la dépendance de scripts complexes pour la sauvegarde.

Huawei

Huawei est l'un des Challengers de ce Magic Quadrant. Le portefeuille de sauvegarde et de protection des données de Huawei comprend le logiciel et les appliances OceanProtect DataBackup, OceanProtect Backup Storage, OceanCyber Data Security Appliance, OceanStor BCManager et Cloud Backup and Recovery. Les opérations de Huawei sont principalement basées

en Asie/Pacifique, EMEA et Amérique du Sud, la majorité de ses clients se trouvant en Asie/Pacifique. Ses clients appartiennent généralement aux segments des moyennes et grandes entreprises. Durant la période d'évaluation, Huawei a lancé OceanProtect DataBackup 1.6.x, comprenant la prise en charge des hyperviseurs Nutanix et Microsoft Hyper-V, Apsara Stack sur Alibaba Cloud, et Microsoft 365 et Entra ID. Il a également commercialisé l'appliance d'architecture évolutive de la série E OceanProtect, ainsi que les appliances de stockage de sauvegarde X3000 et X9000 flash.

Points forts

- **Architecture d'appliance évolutive basée sur le flash :** Huawei propose un portefeuille complet d'appliances de sauvegarde entièrement basées sur la technologie flash. L'ampleur de son portefeuille répond aux attentes des PME comme des grandes entreprises en termes de prix et de performance, tout en offrant les avantages d'une consommation d'électricité réduite, de l'efficacité énergétique et de l'optimisation des performances de sauvegarde et de récupération.

- **Détection des ransomware multicouches :** Huawei intègre sa solution réseau et de stockage pour la détection et le blocage proactifs des cyberattaques. Ses appliances OceanCyber s'intégrant à OceanProtect Backup Storage offrent une protection contre les ransomware.

- **Anonymisation des données lors de la réutilisation des données de copie :** OceanProtect Data Backup permet l'identification des données sensibles et l'anonymisation des copies de sauvegarde de gestion des données de copie.

Réserves

- **Protection multicloud limitée :** les intégrations cloud sans agent Huawei OceanProtect se limitent à la gestion des charges de travail IaaS et PaaS

sur Huawei Cloud, entravant la protection des données et l'optimisation des coûts dans d'autres environnements cloud largement adoptés comme AWS, GCP et Azure.

- **Portée de l'innovation au-delà du portefeuille Huawei :** l'offre BaaS de Huawei se limite au déploiement sur Huawei Cloud, et ses capacités de protection multicouche contre les ransomwarese se cantonnent à l'intégration des composants réseau et stockage de Huawei.

- **Absence de garantie ou d'assurance de récupération après ransomware :** Huawei est en retard par rapport aux leaders du marché en ce qui concerne l'offre d'une garantie ou assurance de récupération après ransomware.

HYCU

HYCU est l'un des Visionnaires de ce Magic Quadrant. HYCU R-Cloud est une plateforme de sauvegarde et de protection des données BaaS hybride et multicloud englobant 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 insights sur les applications et leur statut de protection des données dans les environnements 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 introduit de nouvelles fonctionnalités pour R-Cloud, dont R-Shield pour la détection et la récupération suite à une attaque par ransomware, une couverture étendue à Microsoft Azure Local, et des capacités d'intégration à PowerProtect Data Domain de Dell via l'intégration de DD Boost. Il a également amélioré R-Cloud avec la prise en charge des offres SaaS et PaaS, comme Box, Nutanix Database Service,

Atlassian Bitbucket et Confluence, Microsoft Entra ID, Amazon Virtual Private Cloud, AWS Web Application Firewall et GitLab.

Points forts

- **Stratégie complète de protection SaaS :** reposant sur une méthodologie de développement low-code basée sur l'IA, l'approche de HYCU pour la protection des applications SaaS a permis la création d'une large liste d'applications SaaS prises en charge dans les environnements applicatifs de plusieurs fournisseurs.
- **Solide protection GCP :** HYCU offre une protection complète des services IaaS et PaaS les plus courants de GCP et la prise en charge de Google BigQuery, Firestore, Artifact Registry, Cloud Functions et Cloud Run.
- **BaaS avec stockage sélectionné par le client :** R-Cloud de HYCU, son offre BaaS, permet aux clients de choisir leur propre stockage de sauvegarde, y compris sur site et sur le cloud.

Réserves

- **Segment limité sur le marché des entreprises :** la clientèle d'HYCU comprend essentiellement des entreprises de taille moyenne, peu de déploiements ayant été effectués dans les grandes entreprises, aux environnements diversifiés et complexes à protéger.
- **Retard dans la stratégie de ransomware :** HYCU est en retard par rapport aux principaux fournisseurs en termes de capacités de détection et de réponse aux ransomware. Sa fonctionnalité actuelle R-Shield, basée sur la source et le scan des instantanés, est limitée aux machines virtuelles sur Nutanix. Cette solution n'offre pas la détection des anomalies lors des opérations de sauvegarde, ni de capacités intégrées de recherche de menaces pour l'analyse des données de sauvegarde existantes sans

récupération, ni de scanners antivirus tiers permettant d'identifier les points de récupération les plus sûrs.

- **Limitations de l'intégration cloud native :** R-Cloud exige l'utilisation d'outils tiers pour la protection d'Azure Blob Storage et ne prend pas en charge les conteneurs Azure et AWS multiples, ni les charges de travail PaaS, dont Azure Cosmos DB, Azure SQL Database, Amazon Elastic Kubernetes Service (EKS), Red Hat OpenShift sur AWS et Amazon Elastic Container Service (ECS).

IBM

IBM est l'un des Visionnaires de ce Magic Quadrant. Son portefeuille de sauvegarde et de protection des données comprend IBM Storage Defender, IBM Storage Defender Data Protect et IBM Storage Protect for Cloud. Les opérations d'IBM sont géographiquement diversifiées et ses clients majoritairement de grandes entreprises. Durant la période d'évaluation, IBM a amélioré sa plateforme Storage Defender avec l'ajout d'une intégration protégeant les solutions de stockage IBM FlashSystem et Dell PowerMax. Il a également introduit l'abstraction des policies de récupération pour les applications d'entreprise comme Oracle, SAP HANA et VMware. IBM continue d'améliorer ses capacités d'IA avec watsonx, améliorant ses capacités d'opérations de sauvegarde et de récupération, de résolution des défaillances et d'efficacité.

Points forts

- **Intégration de l'IA :** les modèles et outils d'IA IBM watsonx d'IBM améliorent l'analytics comportemental, la détection d'anomalies en temps réel et les insights spécifiques aux applications pour identifier les cybermenaces via ses capteurs basés sur des agents. Cela améliore l'efficacité opérationnelle et offre des capacités autonomes, comme

l'atténuation des incidents, la planification des capacités et l'allocation des ressources.

- **Intégration de la détection précoce des menaces :** Storage Defender propose la détection en quasi-temps réel des ransomware, en s'appuyant sur plusieurs capteurs répartis sur les machines virtuelles, les systèmes de fichiers, le stockage et certaines applications du client.
- **Génération automatique du groupe de récupération :** Storage Defender orchestre la récupération et applique des policies cohérentes aux charges de travail connexes, à partir d'insights d'actifs protégés de différents snapshots de stockage et copies de sauvegarde.

Réserves

- **Dépendances de produits tiers :** les solutions IBM Storage Defender Data Protect et Storage Protect for Cloud dépendent d'autres fournisseurs pour leur plan produits et de contrôle, le développement du produit échappant ainsi au contrôle d'IBM.
- **Protection multicloud limitée :** Storage Protect for Cloud d'IBM offre une protection limitée des services IaaS et PaaS sur plusieurs clouds, dont AWS, GCP et OCI. Il ne dispose pas de la découverte d'applications cloud et de la récupération d'infrastructure, ni d'options de choix de stockage cloud pour le client.
- **Confusion liée au changement de nom des produits :** les clients d'IBM signalent une confusion et un manque de clarté concernant la cohérence des capacités dans les environnements hybrides, multicloud et SaaS de son portefeuille de sauvegarde et de protection des données.

OpenText

OpenText est l'un des acteurs de niche de ce Magic Quadrant. Son portefeuille de produits de sauvegarde et de protection des données se compose principalement de deux produits : les éditions Data Protector Express et Premium 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. Durant la période d'évaluation, OpenText a amélioré Data Protector avec l'intégration de la détection de logiciels malveillants OpenText Webroot et le lancement de SafeZone Recovery, une analyse sécurisée des sauvegardes. Il a également lancé OpenText Magellan BI & Reporting comme solution de serveur de reporting, la prise en charge d'Impossible Cloud ainsi que des mises à jour de son interface utilisateur Web.

Points forts

- **Ampleur des intégrations de produits OpenText :** OpenText offre une intégration solide grâce à sa solution Webroot de détection des logiciels malveillants, la protection des données OpenText Documentum et des capacités de reporting améliorées grâce à OpenText Magellan BI & Reporting.

- **Protection des applications SaaS :** OpenText propose des options gérées par le client et hébergées par le fournisseur pour la sauvegarde de Microsoft 365. Data Protector for Cloud Workloads prend en charge les déploiements Microsoft 365 gérés par les clients, tandis que la solution hébergée CloudAlly prend en charge Microsoft 365, Salesforce, Google Workspace, Box et Dropbox.

- **Prise en charge étendue des hyperviseurs :** OpenText Data Protector Premium, associé à Data Protector for Cloud Workloads, s'intègre à la

plupart des principaux hyperviseurs. y compris notamment VMware VM, Microsoft Hyper-V, Proxmox Virtual Environment, Red Hat Virtualization, Nutanix AHV, OpenStack, Huawei FusionCompute et Scale Computing HyperCore.

Réserves

- **Aucune solution BaaS hébergée par le fournisseur :** OpenText ne propose pas de solution BaaS axée sur les clients professionnels pour les charges de travail cloud et sur site.
- **La priorité donnée à l'intégration interne affecte l'innovation :** principalement axé sur l'intégration de Data Protector à l'ensemble de sa suite de solutions, OpenText n'a que peu innové dans les domaines émergents du marché des plateformes de sauvegarde et de protection des données.
- **Aucun plan de contrôle basé sur SaaS :** OpenText ne dispose pas d'un plan de contrôle SaaS, ni d'une interface administrative commune pour tous les composants de sa solution, des fonctionnalités fréquemment présentes dans les solutions des principaux fournisseurs.

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

Rubrik

Rubrik est l'un des Leaders de ce Magic Quadrant. Son portefeuille de sauvegarde et de protection des données, Rubrik Security Cloud, comprend plusieurs offres de sauvegarde, de sécurité des données et de récupération avancée. Rubrik propose des solutions de protection des données BaaS par

appliance, 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 ajouté la protection et la prise en charge des données pour Salesforce, Microsoft Dynamics 365, Azure DevOps, GitHub, Microsoft 365 Backup Storage, ainsi que des machines virtuelles et des bases de données sur OCI. Il a également lancé la détection des anomalies et des menaces pour les environnements Azure et AWS, une nouvelle fonctionnalité Turbo Threat Hunting intégrée avec Mandiant Threat Intelligence et la récupération prioritaire pour M365 visant à améliorer la cyberrésilience. Outre ces améliorations, Rubrik a lancé Identity Recovery pour Active Directory et EntraID, et Annapurna de Rubrik pour le développement d'applications GenAI.

Points forts

- **Cyberrécupération et détection robustes :** Rubrik Security Cloud offre des capacités exhaustives de cyber-reprise et de détection pour les données et l'identité. Ces fonctionnalités incluent la détection d'anomalies en ligne basée sur l'IA, la surveillance avancée des menaces et la chasse aux menaces pour l'identification de points de récupération sûrs, et la coordination de la reprise dans des environnements d'identité hybrides.

- **Innovation en matière de stratégie tarifaire :** la licence d'application SaaS universelle de Rubrik prend en charge une capacité de stockage illimitée par utilisateur. Elle est transférable entre toutes les applications SaaS prises en charge par Rubrik.

- **Solution RAG Annapurna GenAI :** Rubrik Annapurna permet aux clients de créer en toute sécurité des applications d'IA générative basées sur les

données de sauvegarde d'entreprise dans Rubrik Security Cloud, avec des contrôles d'accès intégrés et une gestion des données sensibles.

Réserves

- **Couverture géographique limitée :** Rubrik n'attire que peu de clients en dehors de l'Amérique du Nord et de la région EMEA. Cela s'explique par le nombre limité de partenaires actifs dans les autres régions, par rapport à d'autres fournisseurs de premier plan.
- **Pas de récupération inter-hyperviseur :** Rubrik Security Cloud ne prend pas en charge la récupération inter-hyperviseurs dans les environnements de centre de données, ce qui limite sa capacité à gérer des cas d'utilisation comme la reprise après sinistre, la migration et la mobilité des données dans des environnements clients multi-hyperviseurs.
- **Fonctionnalités de reporting limitées :** certains clients ont fait part de leurs préoccupations concernant les fonctionnalités de reporting prêtes à l'emploi, évoquant des capacités limitées, des besoins de personnalisation complexes et la dépendance envers le support de Rubrik pour obtenir une assistance.

Unitrends

Unitrends, une entreprise Kaseya, est l'un des Acteurs de niche de ce Magic Quadrant. Son portefeuille de sauvegarde et de protection des données 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. Durant la période d'évaluation, Unitrends a optimisé l'intégration de son logiciel de sauvegarde

à VMware, réduisant la taille des sauvegardes et mis à jour ses guides produits pour accompagner les utilisateurs dans les tâches courantes. Il a également présenté son nouveau système d'exploitation Alma 9 et l'authentification à deux facteurs pour ses appliances de sauvegarde. Désormais compris dans l'abonnement utilisateur Kaseya 365, Spanning Backup comprend des options de stockage en Afrique du Sud. Ses mises à jour comprennent également l'amélioration des aperçus de récupération pour Microsoft Exchange Online et OneDrive et de nouvelles fonctionnalités, comme la protection illimitée des boîtes aux lettres partagées et l'exportation des mails au format PST.

Points forts

- **Consolidation d'Unitrends et de Datto :** Kaseya a annoncé son intention d'associer Unitrends et son activité Datto. Cette action devrait enrichir le portefeuille disponible pour ses clients.
- **Stockage dans le cloud économique :** Unitrends commercialise un stockage cloud sans sortie pour la conservation à long terme et le stockage hors site. Intégré à son offre DRaaS, celui-ci permet de tester la conformité aux RTO et RPO définis par le client.
- **Forte intégration aux offres Kaseya :** Unitrends UniView fournit la gestion centralisée de son offre de sauvegarde et de récupération, tout en s'intégrant aux solutions de sécurité et de centre de services de Kaseya. L'abonnement utilisateur Kaseya 365 comprend aussi Spanning Backup pour Microsoft 365.

Réserves

- **Adéquation entreprise limitée :** les initiatives de croissance et l'évolutivité limitées des appliances d'Unitrends, principalement axé sur le marché des PME et fournissant ses solutions par l'intermédiaire de fournisseurs

de services gérés, contribuent à réduire son adaptation aux grands comptes d'entreprise.

- **Manque d'expansion des applications SaaS :** Unitrends Spanning Backup n'a ajouté aucune nouvelle charge de travail SaaS durant la période de l'étude. Il ne prend pas en charge les applications SaaS, comme Microsoft Entra ID, Microsoft Dynamics 365, Slack, Box et GitHub.
- **Absence d'IA générative pour les capacités de sauvegarde :** le portefeuille d'Unitrends ne dispose d'aucune fonctionnalité d'IA générative améliorant et simplifiant les tâches administratives de sauvegarde.

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

Veeam

Veeam est l'un des Leaders de ce Magic Quadrant. Ses principales offres de sauvegarde et de protection des données sont Veeam Data Platform (VDP), Veeam Backup pour M365, Veeam Backup pour Salesforce, Veeam Kasten, Veeam Data Cloud (VDC) et Veeam Data Cloud Vault. Les opérations de Veeam sont géographiquement diversifiées, la plupart de ses clients se trouvant dans les segments du marché intermédiaire et des PME. Durant la période d'évaluation, Veeam a publié plusieurs mises à jour de produits, dont VDP v12.3, offrant de nouvelles fonctionnalités comme la prise en charge de Microsoft Entra ID, la détection d'indicateurs de compromission (IOC) et l'analyse proactive des menaces via des outils comme Recon Scanner et Veeam Threat Hunter. Ses principales améliorations sont la prise en charge de l'environnement virtuel Proxmox, des insights basés sur l'IA avec Veeam

Intelligence et la prise en charge des plans de reprise après sinistre Microsoft Hyper-V.

Points forts

- **Présence établie sur le marché :** Veeam bénéficie d'une forte présence sur le marché et d'une large adoption dans toutes les régions du monde, soutenue par un large réseau de partenaires. Cela permet une prestation de services cohérente, une assistance rapide et un accès à l'expertise locale, essentiels pour les entreprises d'envergure internationales.

- **Protection renforcée contre les ransomware et cyberrésilience :** la protection complète contre les ransomware de Veeam comprend l'analyse en ligne basée sur l'IA, Veeam Threat Hunter et la détection IOC. Veeam Cyber Secure, un programme offrant l'assistance aux clients avant, pendant et après les incidents, comprend la garantie de reprise après sinistre en cas de ransomware et apporte une réponse first-party en temps réel aux incidents lors des violations actives.

- **récupération et mobilité polyvalentes des données :** Veeam prend en charge les récupérations inter-hyperviseurs entre les principaux hyperviseurs comme VMware vSphere, Microsoft Hyper-V et Nutanix AHV. Il propose également une fonctionnalité de récupération directe des charges de travail sur site vers AWS, Azure et GCP.

Réserves

- **Approche réactive de l'innovation sur le marché :** les offres et améliorations de Veeam sont généralement lancées en réponse aux offres de la concurrence et à la demande des clients, plutôt qu'en anticipation de celles-ci par des fonctionnalités nouvelles et distinctives sur le marché.

- **Dépendance envers l'infrastructure Microsoft :** Veeam Data Cloud est déployé dans Azure, ce qui pourrait poser problème aux entreprises dépendant principalement d'autres fournisseurs de cloud. De plus, VDC manque de flexibilité pour le stockage des données de sauvegarde dans des emplacements gérés par d'autres fournisseurs de cloud, comme AWS et GCP.

- **Limitation de la protection SaaS :** le portefeuille Veeam ne couvre pas la diversité croissante des applications SaaS en dehors de Microsoft 365, Microsoft Entra ID et Salesforce. Ce qui peut être un problème et un désavantage par rapport aux autres offres pour les entreprises requérant une couverture de protection des données SaaS plus large.

Fournisseurs ajoutés et supprimés

Nous évaluons et modifions nos critères d'inclusion aux Magic Quadrants en fonction de l'évolution du marché. En raison de ces modifications, la liste de fournisseurs étudiés dans un Magic Quadrant peut varier au fil du temps. Si un fournisseur apparaît dans un Magic Quadrant une année, mais pas l'année suivante, cela n'indique pas forcément que nous avons changé d'opinion à son égard. Cela peut refléter une évolution du marché et, par conséquent, des critères d'évaluation, ou un changement d'orientation de la part de ce fournisseur.

Ajoutés

Huawei

Abandonnés

- Microsoft a été exclu de l'étude de cette année, car il ne répondait pas à toutes les exigences obligatoires en matière de fonctionnalités. Son produit Azure Backup ne prend pas en charge la protection des environnements multicloud.

- Veritas a été retiré de l'étude de cette année, car ses produits éligibles ont été associés à Cohesity suite à la conclusion de la transaction de fusion de l'activité de protection des données d'entreprise de Veritas avec Cohesity en décembre 2024.

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 plateforme de sauvegarde et de protection des données du fournisseur doit satisfaire à toutes les fonctionnalités « Obligatoires » définies dans la définition du marché.

- L'exigence multicloud de la plateforme de sauvegarde et de protection des données du fournisseur doit prendre en charge la protection de l'infrastructure en tant que service (IaaS) sur DEUX environnements cloud publics qualifiés pour inclusion dans le Magic Quadrant 2024 des services cloud stratégiques. Ces fournisseurs sont Alibaba Cloud, Amazon Web Services, Google, Huawei Cloud, IBM, Microsoft, Oracle et Tencent Cloud.

- 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 2025 (c'est-à-dire qu'elle doit être disponible sur le marché depuis le 1er avril 2022 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 du prestataire de services gérés (MSP).
    - Le fournisseur doit avoir généré plus de 75 millions d'USD de chiffre d'affaires récurrent annuel (ARR) au 28 février 2025, OU
    - avoir généré plus de 30 millions d'USD de chiffre d'affaires récurrent annuel déclaré au 28 février 2025, ainsi qu'un taux de croissance du chiffre d'affaires récurrent annuel de 20 % en glissement annuel (au 28 février 2024 par rapport au 28 février 2025).
- Le fournisseur doit avoir une clientèle d'au moins 1 000 clients installés sur le marché, telle que définie dans la section 2. 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 assurer activement le support de ses produits de plateforme de sauvegarde et de protection des données sous sa propre marque dans au moins trois des principales régions suivantes : Amérique du Nord, EMEA, Asie/Pacifique et Amérique centrale/du Sud. Au moins 25 % de son chiffre d'affaires récurrent annuel doit provenir de l'extérieur de sa zone géographique principale.
- Le fournisseur doit compter au moins 50 clients générant un chiffre d'affaires, chez lesquels sa plateforme ou solution qualifiante de sauvegarde et protection des données est installée et utilisée en production, dans au moins trois des principales régions suivantes :

Amérique du Nord, EMEA, Asie-Pacifique et Amérique centrale/du Sud. Vingt des 50 clients par zone géographique doivent avoir déployé la solution de sauvegarde pour un minimum de 100 serveurs physiques ou 300 serveurs virtuels. À l'exclusion des sauvegardes de terminaux.

- La/les solution(s) de sauvegarde et de récupération qualifiante(es) du fournisseur doit(vent) être vendue(s) et commercialisée(s) essentiellement auprès des entreprises du marché intermédiaire supérieur et 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 12 derniers mois doivent être disponibles au grand public depuis le 1er avril 2025 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. L'expédition des produits après cette date ne peut avoir qu'une influence sur l'axe de l'Exhaustivité de la vision.

- Le fournisseur doit employer au moins 100 collaborateurs à temps plein, dédiés à sa plateforme de sauvegarde et de protection des données pour l'ingénierie, les vente et le marketing, au 28 février 2025.

Les critères d'exclusion suivants s'appliquent :

- Fournisseurs proposant des produits ou solutions avec des logiciels principalement externalisés auprès d'un ISV tiers.

- Produits servant uniquement de cible ou de destination pour la sauvegarde, mais n'effectuant pas réellement la fonction de gestion de sauvegarde et de récupération. Par exemple les appliances de déduplication sur mesure, le SAN, le NAS et le stockage d'objets.

- Les fournisseurs dont la principale source de revenus produits (plus de 75 % du revenu total) provient de fournisseurs d'hébergement de centres de données et 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, Amazon EC2, Azure Blob, Azure Virtual Machines, 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 qui servent essentiellement à gérer les capacités d'instantané et de réplication des baies de stockage.
- Produits principalement positionnés pour la gestion des données de copie 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. 12 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 de sauvegarde et de protection des données 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.

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 de sauvegarde et de protection des données 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 rencontrés avec le produit

affectant l'expérience client. Les cas d'utilisation des BDPP incluent la protection des environnements sur site hybrides/multicloud et SaaS, les services de données, la reprise après sinistre, ainsi que la protection, la détection et la récupération après attaque de ransomware.

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

Exécution commerciale / tarification : ce critère couvre l'évaluation de la réussite d'un fournisseur sur le marché BDPP. Les éléments pris en compte sont les résultats des activités nouvelles et récurrentes, le nombre de nouveaux clients de sauvegarde et de protection des données et l'évolution des investissements clients dans ses offres. 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 BDPP 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.

Mise en œuvre commerciale : 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 BDPP.

Expérience client : ce critère évalue la capacité du fournisseur à proposer une expérience client positive dans l'utilisation des solutions BDPP. Nous évaluons la capacité à démontrer la satisfaction 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	*Évaluation*
Produit ou service	Élevée
Viabilité globale	Moyenne
Exécution commerciale/tarification	Moyenne
Réactivité sur le marché/antécédents	Élevée
Exécution marketing	Faible
Expérience client	Élevée
Opérations	Non notée

Source : Gartner (juin 2025)

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 exigences des clients pour la sauvegarde et la protection des environnements d'entreprise. Nous évaluons la capacité du fournisseur à s'aligner sur 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 de la BDPP du fournisseur, notamment sa capacité de différenciation concurrentielle et sa connaissance des profils impliqués dans la sélection des solutions de sauvegarde et de protection des données.

Stratégie commerciale : ce critère évalue la capacité du fournisseur à établir et actualiser sa stratégie de vente de BDPP 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 d'offre (produits) : ce critère évalue la planification de l'offre BDPP du fournisseur, en particulier le comblement des lacunes, l'engagement en matière de différenciation et l'amélioration des fonctionnalités existantes, et l'ampleur du recours à des offres OEM ou ISV dans ses produits BDPP.

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

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 et uniques dans la conception de produits de BDPP, le marketing, les ventes et les préventes, ainsi que le support client. Nous évaluons si les innovations les plus récentes et planifiées du fournisseur constitueront une source de valeur pour la clientèle entreprise, si elles sont uniques ou différenciées et si elles représentent un élément restructurant pour le marché BDPP.

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	*Évaluation*
Connaissance du marché	Élevée
Stratégie marketing	Moyenne
Stratégie commerciale	Moyenne
Stratégie de l'offre (produit)	Élevée
Modèle commercial	Moyenne
Stratégie verticale/industrielle	Faible

Critères d'évaluation	*Évaluation*
Innovation	Élevée

Source : Gartner (juin 2025)

Descriptions des Quadrants

Leaders

Les Leaders présentent les scores les plus élevés en termes de Capacité d'exécution et d'Exhaustivité de la vision. Ils disposent des portefeuilles d produits les plus complets et les plus évolutifs, répondant aux exigences sauvegarde et de récupération des environnements IT hybrides, multiclo 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 proprié intellectuelle (PI). Ils disposent aussi de plans élaborés pour l'extension d leurs fonctionnalités générales de récupération et de cyber-récupération 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 environnements IT hybrides 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, avec

des offres et des services généraux qui, à l'heure actuelle, ne sont pas aussi complets que ceux d'autres fournisseurs axés sur le marché des grandes entreprises.

Les Acteurs de niche peuvent se concentrer sur des zones géographiques 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 I&O chargés des opérations de sauvegarde doivent évaluer et repenser leur stratégie de sauvegarde de manière à inclure les facteurs technologies, opérations et consommation appropriés pour leurs entreprises. Leur stratégie doit prendre en compte l’étendue des charges de travail critiques évoluant constamment, l’utilisation du cloud et les exigences de protection accrue des données et de cyberrésilience en :

- Investissant dans des solutions de sauvegarde répondant aux exigences de protection des données des environnements hybrides, multicloud et SaaS. Favorisant les solutions offrant une vision unifiée pour la gestion de ces environnements distribués.
- Choisissant des solutions de sauvegarde incluant une offre native ou intégrée de protection des données de sauvegarde contre les cyberattaques, de détection des anomalies et des logiciels malveillants,

d'alerte en cas d'indicateurs de compromission (IoC) et d'accélération de la récupération suite à une cyberattaque.

- Mettant en œuvre des solutions de sauvegarde et de récupération offrant des principes d'architecture à vérification systématique.
- Optant pour des solutions de sauvegarde basées sur l'IA, comme l'IA générative pour les fonctionnalités de sauvegarde, simplifiant et accélérant les activités d'administration de la sauvegarde, dont la récupération orchestrée.
- Privilégiant les solutions offrant des fonctionnalités de découverte des composants d'infrastructures d'applications cloud, et de test et d'orchestration régulière de la récupération des applications et des données.
- Évaluant le niveau de résilience des copies de sauvegarde, en exigeant la création de plusieurs copies immuables le plus tôt possible dans le processus de sauvegarde.
- Alignant leur architecture de sauvegarde sur les exigences de récupération opérationnelle de l'entreprise. Distinguant les cibles de stockage de la sauvegarde pour utilisation aux fins de récupération opérationnelle, de conservation à long terme et de cyberrécupération.
- 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.
- Sélectionnant des fournisseurs capables d'accroître la valeur des données de sauvegarde au-delà des événements de récupération.

Hiérarchisant les solutions offrant des cas d'utilisation supplémentaires pour les données de sauvegarde. Notamment l'analyse et la classification des données sensibles, les investigations, la prise en charge de l'analytics et de l'enrichissement des données, ainsi que la génération augmentée par la récupération (RAG) et l'accès aux données via API.

Vue d'ensemble du marché

Le marché des plateformes de sauvegarde et de protection des données (BDPP) est la version actualisée du marché des solutions logicielles de sauvegarde et de récupération pour les entreprises existantes. Cette version actualisée tient compte des nouvelles exigences changeantes des entreprises pour leurs besoins de protection de leur vaste et complexe parc de données. Plusieurs facteurs ont influencé l'évolution de la définition du marché et des critères d'évaluation pour l'étude Magic Quadrant et des Attributs critiques de cette année. Les principaux attributs sont :

Plateforme

- Privilégie la gestion centralisée et l'orchestration des plateformes de protection des données.
- Élargit les besoins couverts par la sauvegarde en tant que service (BaaS)
- Opérations de sauvegarde autonomes.
- Étend les cas d'utilisation de la plateforme à la protection des données, la conformité, la gestion des données de copie et aux exigences de test et de développement.
- Étend les fonctionnalités d'analyse et d'accès aux insights de données de sauvegarde, comme la catégorisation et la classification des données, la

détection de données sensibles, la recherche, les investigations, l'analyse décisionnelle (business intelligence), la génération augmentée par la récupération (RAG) et d'autres formes de récupération via API.

Protection des données

- Expansion constante des environnements hybrides, multicloud et SaaS qui doivent être protégés.
- Axée sur la nécessité d'une préparation à la cyberrécupération et de solides capacités de détection des anomalies.
- Capacités émergentes pour effectuer et accélérer la détection des logiciels malveillants dans les données de sauvegarde et les alertes en cas d'incidents de compromission (IoC).
- Découverte, sauvegarde, récupération et reprise après sinistre axées sur les applications.
- Fonctionnalités communes étendues, comme les principes de vérification systématique et l'orchestration étendue de la récupération.

Les fournisseurs de plateformes de sauvegarde et protection des données évalués dans ce Magic Quadrant innovent et modifient le marché dans les domaines suivants :

Capacités de cyber-récupération et de détection

- **Détection et récupération des ransomware :** la plupart des fournisseurs ont développé des capacités de détection des attaques de ransomware en surveillant les anomalies comportementales des données protégées. Ces fournisseurs visent également à simplifier le processus de récupération après attaque par ransomware, en accélérant l'identification du meilleur point de récupération et le plus propre par la création de points de récupération personnalisés, l'association de plusieurs points de

récupération et la création d'un environnement de test et de récupération isolé.

- **Détection des logiciels malveillants :** les fournisseurs ajoutent la détection des logiciels malveillants dans les copies de sauvegarde en association avec des fournisseurs de sécurité ou en développant ces capacités en interne. Ils se distinguent par leur capacité à identifier les variantes connues de ransomware et les attaques zero-day. Les innovations récentes incluent la détection de logiciels malveillants via l'analyse basée sur les règles YARA, l'intégration de flux de données provenant de fournisseurs de sécurité et la chasse avancée aux menaces basées sur le suivi par hachage pour le signalement des indices de compromission (IoC).

- **Stockage hébergé par le fournisseur :** 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 fournisseurs leaders étendent leurs offres en tant que service par la mise en place de services d'orchestration facilitant les tests, le nettoyage et la validation de routine, ainsi que la récupération.

Options d'administration et de déploiement

- **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.

- **Offres BaaS :** les principaux fournisseurs de sauvegarde étendent leurs capacités 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.

- **Options de stockage multicloud :** les fournisseurs étendent leur architecture de plan de données hébergé, offrant aux clients plusieurs options de cible de stockage cloud.

Protection de l'environnement cloud

- **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'ampleur des exigences impose aux fournisseurs de suivre l'évolution croissante des infrastructures IaaS et PaaS, ainsi que la multiplication des emplacements de données dans le cloud.

- **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.

- **Récupération des applications et de l'infrastructure cloud :** les fournisseurs leaders ajoutent des fonctionnalités de découverte de l'infrastructure applicative et des services cloud et l'intégration de leurs propres services, de services tiers ou du cloud public pour la sauvegarde et la protection des applications, les tests et l'exécution du basculement et la restauration de l'ensemble de l'environnement applicatif et des données.

Protection des applications SaaS

- **prise en charge de la protection des applications SaaS :** 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 des applications comme Microsoft Dynamics 365, Microsoft Power Apps, Atlassian Jira et ServiceNow.

- **Sauvegarde et récupération de la gestion des accès et des identités (IAM) :** les fournisseurs ont ajouté des fonctionnalités de sauvegarde et de récupération des données critiques de gestion des accès et des identités. Celles-ci simplifient la protection et la récupération granulaire des offres IAM, comme Microsoft Active Directory, Microsoft Entra ID et Okta. Les dernières avancées comprennent la récupération orchestrée au niveau de la forêt de Microsoft Active Directory, conforme aux meilleures pratiques de Microsoft.

Mise en œuvre de l'IA/ML et de l'IA générative

- **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.

- **Élargir les fonctionnalités de l'IA générative :** les fournisseurs leaders de ce marché n'ont pas tardé à présenter leurs offres de fonctionnalités basées sur l'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, des discussions en langage naturel et des réponses basées sur l'IA. L'utilisation de l'IA générative

devrait conduire à des niveaux d'automatisation élargis, accélérant la récupération et simplifiant l'administration.

- **Émergence de l'IA agentique :** on assiste à l'émergence de capacités des fournisseurs à automatiser les tâches par des agents de sauvegarde. Les capacités actuelles fonctionnent selon un mode basé sur des instructions.

Définitions des critères d'évaluation

Capacité d'exécution

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

Viabilité globale : la viabilité comprend l'analyse de la santé financière globale de l'entreprise, le succès financier et pratique de l'unité commerciale, et la probabilité que l'unité commerciale en question continue à investir dans le produit, à le proposer et à faire avancer la technologie de la gamme de produits de l'entreprise.

Exécution commerciale/tarification : les capacités d'un fournisseur et de la structure compétente pour toutes les activités préliminaires à la vente. dont la gestion des transactions commerciales, de la tarification et de la négociation, de l'assistance technique préliminaire à la vente et de l'efficacité globale du circuit de distribution.

Réactivité du marché/Perception commerciale : l'aptitude à réagir, changer de direction, faire preuve de souplesse et réussir face à la concurrence au gré des opportunités, des actions des concurrents, de l'évolution des besoins des clients 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 favoriser l'image positive du produit/de la marque auprès des acheteurs potentiels. Cette « notoriété » peut résulter d'une série 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 d'utiliser avec succès les produits évalués. Cet aspect comprend spécifiquement la façon dont les clients reçoivent un support technique ou client. Il peut également tenir compte des outils auxiliaires, des programmes de support client (et de leur qualité), de la disponibilité de groupes d'utilisateurs, des accords de niveaux de service (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 de l'entreprise, notamment les compétences, les expériences, les programmes, les systèmes et tous les autres moyens lui permettant d'exercer ses activités 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 répondre concrètement à leurs aspirations

par des produits et services. Les fournisseurs à la vision exhaustive sont à l'écoute des acheteurs et savent comprendre leurs désirs et leurs besoins. Ils peuvent ainsi façonner ou rehausser leurs attentes grâce à leur vision.

Stratégie marketing : ensemble de messages clairs et différenciés communiqués de manière cohérente en interne, puis diffusés au monde extérieur par le biais du site web, de la publicité, de programmes 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 d'offre (produit) : approche du fournisseur pour le développement et la distribution de ses produits. Cette stratégie doit mettre en valeur la différenciation, les fonctionnalités, la méthodologie et les caractéristiques en fonction des besoins actuels et futurs.

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

Stratégie verticale/sectorielle : stratégie du fournisseur d'affectation 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 regroupement, 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, que ce soit de façon directe ou par le biais de partenaires, de canaux et de filiales implantées dans ces autres territoires et marchés.