Guide du marché pour la sauvegarde en tant que service

18 décembre 2024 - ID G00797860 - 19 min de lecture

Par Jason Donham , Michael **Hoeck** et **1 autre**

La sauvegarde en tant que service offre une sauvegarde et une protection des données simplifiées pour protéger les données dans le cloud, sur site ou dans des applications SaaS. Les responsables I&O responsables de la sauvegarde et de la protection des données devraient envisager le BaaS pour compléter et éventuellement remplacer les solutions de sauvegarde sur site.

Aperçu

Principales conclusions

- Le paysage des fournisseurs de sauvegarde en tant que service (BaaS) évolue. Les fournisseurs de sauvegarde d'entreprise traditionnels étendent leurs offres BaaS pour compléter les produits autogérés, augmenter la couverture de la charge de travail et étendre les options de déploiement pour protéger les données des applications hybrides et SaaS.
- L'intérêt des clients pour le BaaS augmente à mesure que de plus en plus d'entreprises informatiques perçoivent les avantages d'un modèle de coût à l'utilisation et qu'elles ont de plus en plus besoin de protéger les charges de travail SaaS, IaaS et PaaS. Les avantages les plus importants sont la nécessité de libérer le personnel informatique pour travailler sur des projets plus difficiles de transformation numérique .
- La présence géographique et les capacités de support varient considérablement selon les fournisseurs BaaS. Par conséquent, certains fournisseurs BaaS s'appuient sur des

fournisseurs de services gérés et des revendeurs régionaux pour héberger, intégrer et assister les clients .

- Les fournisseurs BaaS augmentent leur gamme de support pour les hyperviseurs alternatifs , tels que Nutanix AHV, Red Hat OpenShift et d'autres hyperviseurs basés sur KVM.
- Les offres des fournisseurs de BaaS varient en termes de maturité des capacités de détection, de réponse et de récupération des ransomwares.

Recommandations

- Assurez-vous que la bande passante réseau disponible est suffisante pour sauvegarder les données sur le stockage du fournisseur avant de passer à la solution BaaS. Pour les environnements plus vastes, utilisez un logiciel de sauvegarde d'entreprise pour fournir des services .
- Donnez la priorité à B aaS pour protéger les applications SaaS à grande échelle ou critiques, telles que Microsoft 365, Microsoft Entra ID et Salesforce .
- Sélectionnez les fournisseurs BaaS dont les capacités s’adaptent le mieux aux charges de travail sur site et dans le cloud des clients, aux exigences de souveraineté des données et aux accords de niveau de service (SLA).
- Développer un modèle complet de coût total de possession (TCO) BaaS en garantissant une compréhension approfondie des structures de frais de sortie pour la récupération des données depuis le cloud, y compris les transferts de données cloud à cloud .
- Privilégiez les fournisseurs BaaS qui proposent une plateforme unifiée pour protéger les environnements cloud IaaS, PaaS et SaaS en plus des machines virtuelles (VM), des applications et des données de fichiers hébergées sur site .
- Améliorez la cybersécurité en sélectionnant des solutions BaaS dotées de solides capacités de protection, de détection et de récupération des ransomwares qui s'alignent étroitement sur les types d'applications protégées.

Hypothèses de planification stratégique

- D'ici 2028, 75 % des grandes entreprises adopteront la sauvegarde en tant que service (BaaS), parallèlement aux outils sur site, pour sauvegarder les charges de travail dans le cloud et sur site, contre 15 % en 2024.
- D'ici 2028, 75 % des entreprises donneront la priorité à la sauvegarde des applications SaaS comme une exigence critique, contre 15 % en 2024.
- D’ici 2028, 90 % des produits de sauvegarde et de restauration d’entreprise incluront une technologie intégrée pour détecter et identifier les cybermenaces, contre moins de 45 % en 2024.

Définition du marché

Ce document a été republié le 19 décembre 2024. Le document que vous consultez est la version corrigée. Pour plus d'informations, consultez la page sur gartner.com.

Les fournisseurs BaaS fournissent la protection des données en tant que service en hébergeant le logiciel de sauvegarde et le référentiel de sauvegarde principal dans des centres de données privés ou publics . L'infrastructure de sauvegarde, y compris le logiciel de sauvegarde, les serveurs de sauvegarde et le stockage, est gérée par le fournisseur BaaS. Les clients sont toujours responsables de la mise en œuvre des politiques de sauvegarde et de l'exécution des tâches de récupération, mais ne sont pas responsables de la maintenance et du fonctionnement quotidiens du système de sauvegarde.

Description du marché

Les fournisseurs BaaS protègent principalement l'infrastructure cloud et les données d'application dans les environnements IaaS, PaaS et SaaS. Certains fournisseurs étendent les fonctionnalités pour protéger les machines virtuelles, les bases de données et les systèmes de fichiers sur site.

Les solutions BaaS protègent les types de charges de travail suivants :

- Applications SaaS , telles que Microsoft 365 , Salesforce, Atlassian (Jira) et ServiceNow
- Instances IaaS de cloud public , telles qu'Amazon Elastic Compute Cloud (Amazon EC2), Google Virtual Private Cloud (VPC) et VMware Cloud Foundation (VCF)

- Services PaaS de cloud public , tels que Cloud Foundry, Microsoft Azure DevOps et Red Hat OpenShift
- Machines virtuelles et bases de données hébergées sur site

Le mode de fonctionnement de base est similaire pour tous les fournisseurs BaaS ; cependant, il existe des domaines dans lesquels un fournisseur BaaS peut se distinguer :

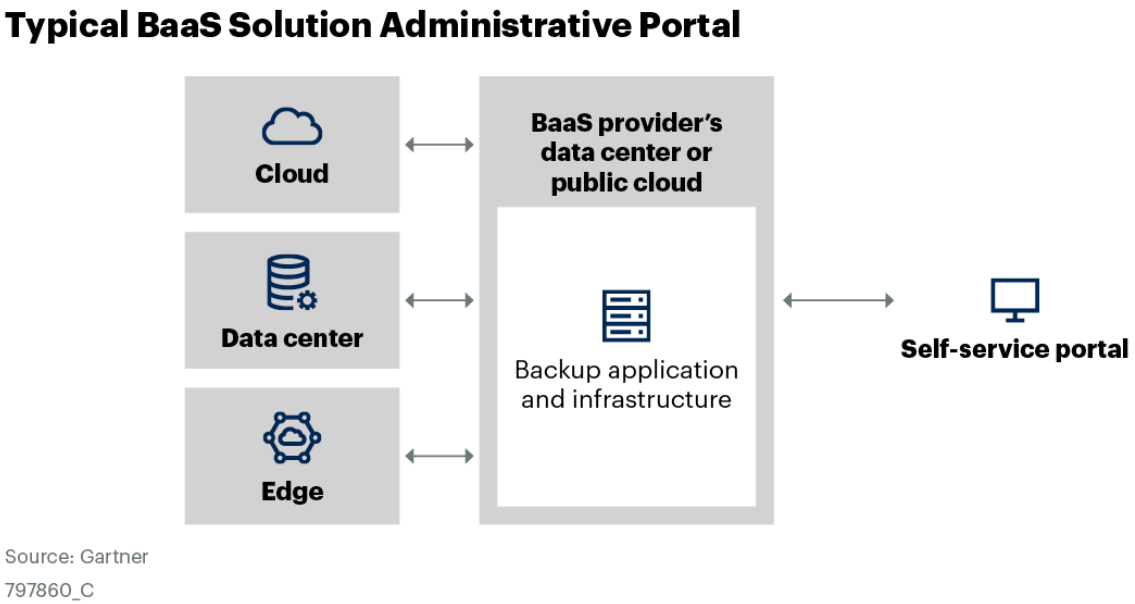
- De nombreux fournisseurs BaaS peuvent accélérer la sauvegarde complète initiale vers le centre de données cloud. Cela peut être effectué en expédiant physiquement des disques durs externes au fournisseur BaaS ou en exploitant les services de transfert de données en masse du fournisseur de cloud public.
- Les centres de données gérés par le cloud ou par un fournisseur constituent un emplacement pratique pour la sauvegarde des données. Toutefois, les restaurations de masse peuvent être lentes. Pour résoudre ce problème, de nombreux fournisseurs de BaaS prennent en charge le stockage de copies de sauvegarde plus récentes sur le stockage local du site client.
- Le chiffrement des données de sauvegarde est standard. Cependant, certains fournisseurs proposent également la possibilité d'apporter votre propre clé et de faire tourner les clés de chiffrement . De plus, les données de sauvegarde sont stockées dans le contexte de sécurité du fournisseur afin qu'une faille de sécurité sur le site du client ne permette pas à l'attaquant de supprimer ou de corrompre les sauvegardes.
- Certains fournisseurs BaaS offrent une capacité de restauration en libre-service permettant aux clients d'effectuer des actions de récupération sans avoir à contacter au préalable le fournisseur BaaS pour obtenir de l'aide .
- Les fournisseurs de BaaS proposent un type de tableau de bord permettant de suivre l'activité de sauvegarde, la réussite/l'échec des tâches de sauvegarde, la consommation de stockage et le coût. Certains fournisseurs proposent des rapports avancés dans le cadre de leur solution BaaS, tels que des rapports détaillés personnalisables, des analyses et des visualisations de données et de sauvegarde, des analyses prédictives, une planification de la capacité et des analyses de métadonnées.
- Certains fournisseurs proposent des services supplémentaires tels que la découverte électronique, l'archivage, l'analyse de sécurité des sauvegardes pour détecter les logiciels

malveillants intégrés, la détection des anomalies de ransomware, l'analyse des données sensibles et l'accès aux données de l'IA générative (GenAI).

- Apportez votre propre stockage (BYOS), un centre de données hébergé par le fournisseur, plusieurs options de cibles cloud et une hiérarchisation des données pour réduire les coûts pour les clients.
- Certains fournisseurs proposent des solutions de coffre-fort sécurisé immuable pour leurs copies de sauvegarde de données sur site ou dans le cloud public. Ces solutions offrent une garantie d'immuabilité, de protection contre les fuites d'air et de récupération des données protégées.

La figure 1 représente un portail administratif de solution BaaS typique.

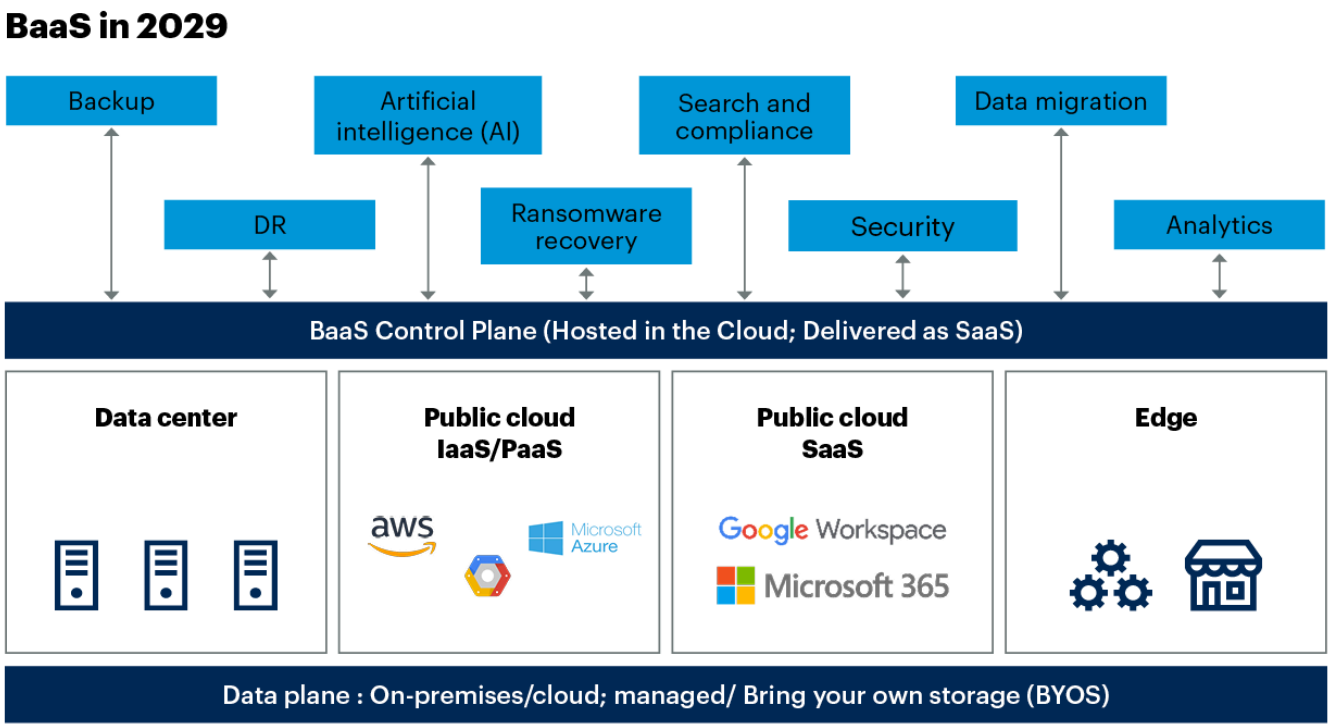
Figure 1 : Portail administratif d'une solution BaaS typique



Orientation du marché

Le paysage des fournisseurs BaaS évolue rapidement, à mesure que les fournisseurs de sauvegarde de centres de données et les nouveaux acteurs s'efforcent de se différencier de leurs concurrents . La figure 2 illustre la vision à long terme des fournisseurs BaaS.

Figure 2 : Orientation du marché des fournisseurs BaaS



Source: Gartner
797860_C

Gartner

Certains fournisseurs ont découplé le plan de contrôle de sauvegarde et le plan de données , ce qui permet aux clients de stocker les données à proximité des applications sans nécessiter que le plan de contrôle existe à plusieurs endroits. Cela garantit que les besoins de protection et de conservation des applications sont satisfaits, quel que soit l'emplacement (sur site, en périphérie ou dans le cloud public).

Les fournisseurs d'entreprise traditionnels considèrent également le plan de contrôle comme un outil unique de gestion des services de sauvegarde et de récupération dans l'ensemble de l'entreprise, qu'ils soient basés sur des déploiements sur site traditionnels ou sur BaaS. Le plan de contrôle consolidé fournira une vue de toutes les copies de sauvegarde, permettant des cas d'utilisation supplémentaires tels que la reprise après sinistre (DR), la récupération après ransomware, la recherche et la conformité et la migration de données, comme illustré dans la figure 2.

De plus, les API exposées par le plan de contrôle permettront à des tiers de fournir des services de données supplémentaires sur la plateforme BaaS.

Le plan de données où sont stockées les données de sauvegarde doit être à proximité immédiate de l'environnement de production pour une récupération rapide. Pour les applications de production hébergées dans le centre de données (sur site) ou en périphérie, une copie de sauvegarde locale doit être stockée sur site, soit dans une appliance physique

ou virtuelle fournie par un fournisseur BaaS, soit sur un système de stockage tiers . Une deuxième copie est généralement stockée dans le cloud pour la reprise après sinistre.

Pour une protection supplémentaire contre les cyberattaques, la plupart des fournisseurs de BaaS rendent impossible la suppression des copies de sauvegarde dans le cloud à l'aide du compte du client ou fournissent des services de coffre-fort isolés supplémentaires. Pour les applications hébergées dans le cloud public, les copies de sauvegarde sont stockées dans des référentiels de stockage d'objets dans le cloud.

Les tendances du secteur comprennent :

- Les fournisseurs de sauvegarde d'entreprise ajoutent des fonctionnalités à leurs plateformes BaaS .
- Les fournisseurs de BaaS proposent des services complémentaires.
- Les fournisseurs autorisent le BYOS comme alternative au stockage géré .
- La confidentialité, la souveraineté et la propriété des données sont des préoccupations dans les secteurs réglementés.

Les fournisseurs de sauvegarde d'entreprise ajoutent des fonctionnalités à leurs plateformes BaaS

Les fournisseurs de sauvegarde d'entreprise traditionnels ont commencé avec des offres BaaS très limitées, telles que la prise en charge de Microsoft 365. Ces fournisseurs élargissent ces offres avec la prise en charge d'une variété de sources de données, notamment les applications sur site, le cloud IaaS, le cloud PaaS et des applications SaaS supplémentaires.

Les fournisseurs BaaS proposent des services complémentaires

En plus de la sauvegarde/restauration, les fournisseurs de BaaS proposent d'autres services , notamment :

- Des copies isolées de sauvegarde et d'analyse des logiciels malveillants sont des composants de plus en plus courants des services BaaS.
- Restaurez les applications sauvegardées sur une cible dans le centre de données cloud public/BaaS.

- Hiérarchisez les données de sauvegarde plus anciennes vers des niveaux de stockage cloud moins coûteux, tels qu'Amazon S3 Glacier ou Azure Archive Storage.
- Une autre copie des données de sauvegarde est isolée de tout accès sur site qui pourrait conduire à la suppression ou au chiffrement des données de sauvegarde.
- Migrez les applications sur site vers le cloud public.
- Utilisez les ressources cloud pour analyser les sauvegardes à la recherche de logiciels malveillants et aider à la détection des attaques de ransomware.
- La copie des données dans le cloud , associée à la reprise après sinistre dans le cloud en tant que service (DRaaS), à l'analyse des logiciels malveillants et à l'automatisation de la récupération, peut fournir des capacités de récupération de ransomware sophistiquées, en particulier pour les petites organisations.
- Créez des copies supplémentaires de données de sauvegarde pour exécuter des projets d'analyse ou de test/développement et faire apparaître des données via l'invite et la réponse GenAI.
- Exécutez des audits périodiques sur les données de sauvegarde indexées pour garantir la conformité ou prendre en charge les processus de découverte électronique .

Les fournisseurs autorisent le BYOS comme alternative au stockage géré

Certains fournisseurs de BaaS offrent la possibilité d'utiliser le compte cloud public du client pour stocker les données de sauvegarde. Toutefois, lors du calcul du coût total de possession pour BYOS , les clients doivent prendre en compte les éléments suivants :

- L'impact des coûts de sortie du cloud public lors de la récupération des données
- L'incapacité à tirer parti des accords de stockage à bas prix que les fournisseurs de BaaS peuvent être en mesure de conclure avec les principaux fournisseurs de cloud public
- La possibilité que les sauvegardes sur BYOS puissent être exposées si le compte cloud du client est piraté

La confidentialité, la souveraineté et la propriété des données sont des préoccupations dans les secteurs réglementés

Les agences gouvernementales, les établissements de défense et les entreprises qui font partie des secteurs réglementés (tels que les services de santé, d'assurance et financiers)

continuent de faire preuve de prudence lorsqu'elles évaluent la sauvegarde dans le cloud. Les préoccupations relatives à la souveraineté, à la confidentialité et à la propriété des données sont quelques-uns des obstacles qui obligent ces entreprises à continuer d'utiliser des solutions de sauvegarde hébergées sur site .

Analyse de marché

Le marché BaaS a commencé avec une focalisation sur la protection des terminaux, suivie par l'ajout de la sauvegarde SaaS et plus récemment de l'ensemble de l'infrastructure client. Les fournisseurs de logiciels de sauvegarde et de récupération d'entreprise ont connu une expansion rapide des services BaaS au cours des cinq dernières années. Les entreprises appliquent une approche plus stratégique pour protéger l'infrastructure cloud et équilibrer l'utilisation de BaaS et les déploiements gérés par le client dans le cadre de la stratégie.

Gartner constate une adoption croissante du BaaS par des entreprises de toutes tailles et de tous secteurs verticaux pour trois cas d'utilisation :

- Protection des applications SaaS : Les clients de Gartner reconnaissent de plus en plus la nécessité de protéger les données stockées dans les applications SaaS, telles que Microsoft 365 et Salesforce.
- Protection des données stockées dans les composants IaaS et PaaS : À mesure que les organisations étendent leur utilisation des offres IaaS et PaaS, telles que les bases de données dans les principaux clouds publics, elles reconnaissent la nécessité d'une meilleure protection des données.
- Protection des bureaux distants : BaaS offre un moyen relativement simple de protéger les données dans les bureaux distants sans nécessiter d'expertise locale.

Représentants des fournisseurs

Les fournisseurs mentionnés dans ce guide du marché ne constituent pas une liste exhaustive. Cette section vise à fournir une meilleure compréhension du marché et de ses offres.

Le tableau 1 présente un échantillon représentatif de fournisseurs proposant des services BaaS . Ces fournisseurs sont soit fréquemment cités dans les demandes de renseignements des clients, soit des fournisseurs majeurs sur ce marché.

Tableau 1 : Fournisseurs représentatifs de BaaS

Veritas fait désormais partie de Cohesity	Veritas Alta, plateforme de gestion de données cloud : Veritas Alta BaaS, Veritas Alta SaaS Protection	Non	Non	Azure SQ Azure Managed SQL, Azu mySQL, A Database pour PostgreS Azure Database pour Mari Amazon DynamoD

Source : Gartner (décembre 2024)

Sélection du fournisseur

Le paysage des fournisseurs BaaS peut être largement classé en deux segments :

- Il s'agit de fournisseurs BaaS qui possèdent leur propre plateforme logicielle de sauvegarde et qui s'appuient généralement sur un fournisseur de cloud hyperscale, tel qu'AWS, Microsoft Azure ou Google Cloud Platform, pour héberger la plateforme et le stockage de sauvegarde. Dans certains cas, les fournisseurs BaaS utilisent un centre de

données de colocation pour héberger l'infrastructure de sauvegarde , souvent pour prendre en charge les zones géographiques où un centre de données cloud n'est pas disponible. Les clients peuvent acquérir des services directement auprès du fournisseur ou via un partenaire fournisseur de services.

- Outre la gamme croissante d'offres BaaS des fournisseurs de sauvegarde établis, de nombreux nouveaux fournisseurs proposent une variété de services BaaS. Certains fournisseurs se concentrent encore entièrement sur les applications SaaS ou cloud telles que Microsoft 365. Cependant , la majorité de ces fournisseurs proposent désormais une gamme de services, notamment la sauvegarde des applications SaaS, la sauvegarde des charges de travail cloud et la sauvegarde des charges de travail sur site.

Recommandations du marché

Les responsables I&O axés sur l'infrastructure, les opérations et la gestion du cloud doivent :

- Sélectionnez des fournisseurs BaaS capables de protéger toutes les charges de travail qu'ils doivent protéger, telles que les machines virtuelles sur site, les bases de données, les fichiers, les charges de travail IaaS et SaaS du cloud public. Si possible, choisissez la solution qui offre la prise en charge la plus large pour les charges de travail à protéger, à moins que des exigences spécifiques en matière de sauvegarde des applications ne nécessitent une solution ponctuelle.

- Sélectionnez des fournisseurs BaaS pour la sauvegarde des charges de travail sur site qui peuvent stocker une copie locale des données de sauvegarde afin de réduire l' objectif de temps de récupération (RTO) et de minimiser les coûts de bande passante.

- Analysez l’impact du modèle de tarification de chaque fournisseur sur le coût total de possession avant de sélectionner un fournisseur BaaS.

- Sélectionnez un fournisseur BaaS en fonction de sa capacité à protéger les données de sauvegarde et l'infrastructure BaaS sous-jacente contre les attaques de ransomware. Connaissez les rôles et responsabilités du client et du fournisseur BaaS, ainsi que les risques associés en cas d'attaque de ransomware sur l'infrastructure de sauvegarde.

- Assurez-vous que l'équipe de gestion des risques et de la conformité examine les conditions générales du fournisseur BaaS pour garantir que les risques associés à la

confidentialité, à la propriété, au cryptage et à la souveraineté des données sont bien compris.

- Déterminez les conséquences d'une interruption de service et le rôle du fournisseur BaaS lors de tels événements. Incluez l'équipe juridique lors de l'examen du SLA du fournisseur.
- Évaluez les conditions du fournisseur concernant l’accès aux données sauvegardées s’il quitte le fournisseur.

Note 1 : Couverture initiale du marché par Gartner

Ce guide du marché fournit la couverture initiale du marché par Gartner et se concentre sur la définition du marché, la justification du marché et la dynamique du marché.