Market Guide for Backup as a Service

Published 18 February 2021 - ID G00727733 - 12 min read
By Analysts Santhosh Rao, Nik Simpson

Initiatives: Cloud and Edge Infrastructure; Data Center Infrastructure

The backup-as-a-service market is poised for rapid growth, driven by ease of use and convenient consumption models. I&O leaders responsible for backup operations of midsize IT infrastructure can simplify backup operations and reduce the infrastructure footprint with cloud-based backup as a service.

Overview

Key Findings

- The backup as a service (BaaS) vendor landscape is rapidly evolving, with providers offering a varying range of capabilities and deployment options with increased focus on public cloud backup.

- Due to the differences in capabilities, consumption models and architecture between on-premises backup and BaaS solutions, enterprises are unable to ascertain the total cost of ownership of BaaS solutions.

- Geographical presence and support capabilities vary significantly among BaaS vendors and continue to evolve. As a result, BaaS vendors rely on service providers and resellers to onboard and support customers.

- As enterprises continue to migrate applications to the public cloud, protecting applications in the cloud continues to be an afterthought, or not considered when selecting a BaaS provider.

Recommendations

I&O leaders focused on cloud and edge infrastructure must:

- Evaluate BaaS solutions for midsize on-premises IT environments that require the protection of fewer than 100 VMs and 25TBs of file data. For larger environments, select BaaS hosters that use enterprise backup software to deliver services.

- Select BaaS providers that meet business RTO requirements and minimize cost by thoroughly evaluating needs for local on-premises backup copies and gaining a complete understanding of egress charges to recover data from the cloud.
Select the BaaS provider based on local cloud data center availability, SLAs and types of services offered.

Choose BaaS providers that offer a unified platform to protect cloud IaaS, PaaS and SaaS environments in addition to VMs, applications, and file data hosted on-premises and endpoints.

Market Definition

BaaS providers deliver data protection as a service by hosting the backup software and the primary backup repository in the provider’s data center or a hyperscale public cloud. The backup infrastructure, including backup software and backup servers and storage, is managed by the BaaS provider. Backup and recovery tasks continue to be performed by the customer by accessing the backup portal hosted in the cloud. The service is usually delivered as a subscription.

BaaS providers primarily protect VMs, databases and files hosted on-premises as well as in the public cloud. Additionally, BaaS providers can offer backup of SaaS applications, such as Microsoft Office 365 and Google Workspace, as well as endpoints.

This report does not include BaaS providers that only support backup of endpoints or only SaaS applications, such as Microsoft Office 365 or Salesforce.

Market Description

While the use cases supported and capabilities offered by BaaS solutions are not as comprehensive as enterprise data center backup and recovery solutions, they usually protect the following types of workloads:

- VMs, databases and files hosted on-premises
- Public cloud IaaS instances
- SaaS applications such as Microsoft Office 365
- Endpoints

The core attributes of BaaS providers are similar to on-premises backup solutions. The following are some of the key attributes of a BaaS platform.

**Initial seed transfer:** Most BaaS providers offer an option to perform the initial base transfer of the full backup copy to the cloud data center. This can be performed by physically shipping external hard drives to the BaaS provider’s data center or by leveraging the bulk data transfer services of the public cloud provider.

**Local backup copy:** Most BaaS providers offer an option for storing recent copies of backup data on-premises for quick recovery. Recent backup copies can be stored on-premises on commodity hardware.
Security: Backup data is usually encrypted when it is transferred from on-premises to the public cloud. Backup data is encrypted and stored in a secure multitenant cloud environment. Some vendors offer role-based access control, so different users within the organization can manage specific recovery processes.

Self-service: BaaS providers usually provide a self-service portal to perform common administrative tasks, such as downloading and installing client agents and protecting and recovering systems.

Reporting: The self-service portal offered by the BaaS vendor also provides a dashboard to track backup activity, storage consumption and cost.

Termination: Upon termination of the contract, BaaS providers usually offer 30 to 60 days to copy backup data to an alternate provider. This can be performed by physically shipping hard drives to a BaaS provider’s data center or by leveraging the bulk data transfer services of the public cloud provider.

Figure 1 represents a typical BaaS solution architecture.

Market Direction

The BaaS vendor landscape is rapidly evolving, as both data center backup vendors and new players continue to add new capabilities in order to differentiate themselves from competition. Figure 2 depicts the long-term vision of BaaS providers. Gartner anticipates that the backup control plane and data plane will be decoupled over a period of time. This will ensure the protection and retention needs of applications are addressed, irrespective of location — on-premises, edge or the public cloud. The BaaS
control plane will provide a single pane of glass for managing backup and recovery services across the enterprise. Since the BaaS control plane provides a consolidated view of all backup copies, it can enable additional use cases such as disaster recovery (DR), archiving, search and compliance, copy data management, and data migration, as shown in Figure 2.

The data plane that stores the backup copies should be in close proximity to the production environment for quick recovery. For production applications hosted in the data center (on-premises) or at the edge, a local backup copy is stored on-site, either in a BaaS-vendor-provided appliance or on a third-party storage system. A second copy is usually stored on the cloud for DR or recovery in the cloud. For applications hosted in the public cloud, the backup copies are stored in object storage repositories in the cloud.

The following are some of the industry trends.

**BaaS Providers Are Offering Add-On Services**

In addition to just backup/restore, BaaS providers are beginning to offer one or more of the following add-on services:

- Disaster recovery — Restore backed-up applications onto a target in the public cloud/BaaS data center.
Pricing Models Differ Significantly Between BaaS Providers

The pricing for protected data varies from vendor to vendor. Per-instance and per-TB pricing models are the most common. Some vendors charge per front-end TB per month, whereas others charge per back-end TB (after deduplication) per month. Pricing models for protecting endpoints and SaaS applications, such as Microsoft 365, are consistent across vendors and are usually charged on a per-user per-month consumption model.

Vendors Are Allowing BYOS as an Alternative to Managed Storage

Certain BaaS providers offer the flexibility of using the customer’s own public cloud account for storing backup data. However, such customers must factor in the impact of public cloud egress costs during data recovery when calculating the total cost of ownership. Customers that leverage storage that is managed by BaaS vendors directly do not deal with this risk, as the BaaS provider pays for egress costs.

Data Privacy, Data Locality and Ownership Are Concerns in Regulated Industries

Government agencies, defense establishments and enterprises that are part of regulated industries (such as healthcare, insurance and financial services) continue to be conservative and exercise caution when evaluating cloud backup. Concerns on data locality, privacy and ownership are some of the inhibitors that force such enterprises to continue using on-premises-hosted backup solutions.

Market Analysis

Gartner client inquiries indicate that a majority of customers that invest in BaaS offered by backup vendors are midsize enterprises that operate an environment consisting of less than 100 VMs and 25TB of application and file data. Operational simplicity, self-service and opex-based consumption are the key drivers for such enterprises to invest in BaaS solutions.

While BaaS offerings from backup vendors are preferred by midsize enterprises, we observe that large enterprises are increasingly considering BaaS offered by hosters. Since BaaS hosters partner with

---

- Archiving — Tiering older backup copies to a low-cost cloud storage tier, such as tape or object storage, archiving application, and/or data for compliance reasons.
- Data migration — Migrate on-premises applications to the public cloud.
- Ransomware detection and recovery services — Detect ransomware attacks on clients or backup data and facilitate the recovery process.
- File storage — File storage repository.
- Copy data management — Create additional copies of backup data for executing analytics or test/development projects.
- Compliance — Running periodic audits on indexed backup data to ensure proactive compliance or support e-discovery processes.
traditional enterprise data center backup vendors, the solutions offered are much more comprehensive and considered enterprise-grade. Typically, BaaS hosters deploy backup software and backup storage systems in the customer's data center. Data is backed up to this backup storage system and is used for short-term operational recovery. A second copy of backup data is replicated to the backup hoster's data center, and usually an archive copy is vaulted to tape for off-site storage. BaaS hosters provide the customer with a self-service portal for application recovery and usage tracking. In some cases, managed recovery is offered as an additional service. While the solution from BaaS hosters appears comprehensive, a majority of BaaS hosters have limited recovery experience.

Representative Vendors

Market Introduction

The BaaS vendor landscape can be broadly categorized into two segments (see Tables 1 and 2):

- Backup vendors offering BaaS: BaaS providers that own their own backup software platform and leverage a hyperscale cloud provider such as AWS, Microsoft Azure or Google Cloud Platform to host the platform and backup storage. In some cases, BaaS providers use a colocation data center to host backup infrastructure. Customers can leverage services either directly or via a service provider partner.

- BaaS hosters: BaaS providers that partner with enterprise backup solution vendors, such as Dell Technologies, Commvault, Veritas and Veeam, and offer data protection services using these platforms. The underlying infrastructure is often owned and managed by the BaaS hoster. Typically, a BaaS hoster offers other hosting services.
Table 1: Backup Vendors Offering BaaS

Viewing partial table. Click here to view full table

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product</th>
<th>VM (VMware/Microsoft Hyper-V)</th>
<th>Containers</th>
<th>Database (Oracle and Microsoft SQL Server)</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>AISHU</td>
<td>AnyBackup</td>
<td>VMware and Microsoft Hyper-V</td>
<td>No</td>
<td>Oracle and Microsoft SQL Server</td>
<td>Yes</td>
</tr>
<tr>
<td>Acronis</td>
<td>Acronis Cyber Protect</td>
<td>VMware and Microsoft Hyper-V</td>
<td>Yes (Virtuozzo)</td>
<td>Oracle and Microsoft SQL Server</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Source: Gartner (February 2021)
Table 2: BaaS Hosters

<table>
<thead>
<tr>
<th>Region</th>
<th>Representative BaaS Hosters</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>CenturyLink, Flexential, iLand, INAP, TELUS</td>
</tr>
<tr>
<td>Latin America</td>
<td>CenturyLink, ASSET Technology Group</td>
</tr>
<tr>
<td>Europe</td>
<td>CenturyLink, AntemetA, iLand, INAP</td>
</tr>
<tr>
<td>Middle East and Africa</td>
<td>BIOS Middle East, Etisalat Group, Alpha Data, Midis Group, Oman Data Park, Cloud4C</td>
</tr>
<tr>
<td>China</td>
<td>CITIC Telecom CPC</td>
</tr>
<tr>
<td>Japan</td>
<td>INAP, NS Solutions, NTT Communications</td>
</tr>
<tr>
<td>Rest of Asia/Pacific</td>
<td>CITIC Telecom CPC, CloudRecover, Cloud4C, iLand, NTT-Netmagic, Telstra, Sify, Singtel, Logicalis</td>
</tr>
</tbody>
</table>

Source: Gartner (February 2021)

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Recommendations

I&O leaders focused on infrastructure, operations and cloud management must:

- Select BaaS providers on their ability to provide a backup solution addressing data protection requirements of on-premises VMs, databases, files, public cloud IaaS and SaaS workloads. Avoid multiple point-based BaaS products.

- Select BaaS providers that offer an option to store a local copy of backup data in order to reduce RTO and minimize bandwidth costs.

- Analyze the impact of storage pricing models (front-end or back-end storage), storage tiering, retention period, data egress and bandwidth on the total cost ownership before selecting a BaaS provider.
Select a BaaS provider based on the ability to protect backup data and underlying BaaS infrastructure from ransomware attacks. Understand the roles and responsibilities of the customer and the BaaS provider and associated risks in the event of a ransomware attack on the backup infrastructure.

Thoroughly understand the terms of exit, cost and ability of the BaaS provider to move backed-up data in bulk, in a readable format, to their new provider. Switching to an alternative BaaS provider is a complex process.

Ensure the terms and conditions of the BaaS provider are reviewed by the risk and compliance team to ensure risks associated with data privacy, data ownership and data locality are well understood.

Understand the consequences of service disruption and the role of the BaaS provider during such events. Include the legal team when reviewing the provider SLA.

Note 1: Representative Vendor Selection
The list of representative vendors were sourced from Gartner secondary research.

Note 2: Gartner’s Initial Market Coverage
This Market Guide provides Gartner’s initial coverage of the market and focuses on the market definition, rationale for the market and market dynamics.

Document Revision History
Market Guide for Backup as a Service - 4 May 2020

Recommended by the Authors
Magic Quadrant for Data Center Backup and Recovery Solutions
Critical Capabilities for Data Center Backup and Recovery Solutions
Prevent Data Loss by Assessing Your Office 365 Backup and Recovery Needs
Streamline and Simplify Salesforce Backup and Recovery
Top 5 Emerging Cost Optimization Opportunities for Storage and Data Protection
Hype Cycle for Storage and Data Protection Technologies, 2020
2020 Strategic Roadmap for Storage
How Markets and Vendors Are Evaluated in Gartner Magic Quadrants