IDC

SPOTLIGHT

Sponsored by: HPE

Backup as a service is one of the fastest-growing data protection markets. It has the potential to help organizations achieve more complete data protection, reduce staff effort, and lower the cost of protecting data.

Using Backup as a Service to Modernize Data Protection

December 2022

Written by: Phil Goodwin, Research Vice President, Infrastructure Systems, Platforms, and Technologies Group

Introduction

Data backup operations are foundational to data availability, digital resilience, data governance, and digital transformation. Properly managed and configured, backup ensures data survival in the face of any loss scenario. Organizations today deal with incredibly complex environments with data spread across the core, cloud, and edge. In fact, about 48% of data is at the core, 29% in the cloud, and 19% at the edge, with the remaining 4% in "other" locations. While data is growing the fastest in the cloud and at the edge, organizations will be protecting on-premises and hybrid workloads for years to come. This protection must cover any operating platform, application, file system, or database.

Currently, most organizations use hybrid cloud and more than 90% leverage the cloud for data protection. Moreover, IDC predicts that by 2025, 55% of organizations will adopt a cloud-centric data protection strategy. This means that although organizations must protect workloads across the enterprise, they will do so using cloud principles and technologies that deliver high degrees of agility and better service-level agreements (SLAs).

AT A GLANCE

WHAT'S IMPORTANT

IDC predicts that by 2025, 55% of organizations will adopt a cloud-centric data protection strategy.

KEY TAKEAWAYS

Backup as a service (BaaS) is among the fastest-growing data protection markets (19.1% CAGR, according to IDC forecasts). BaaS has the potential to:

- » Reduce IT staff workload
- » Leverage cloud economics for lower TCO
- » Simplify backup operations
- » Improve data governance

Backup as a service (BaaS) is one of the fastest-growing data protection markets. This growth is driven by an increase in cloud-related spending, the root of which is more cloud application deployments. In fact, IDC estimates that 80% of new application deployments are in the cloud. BaaS involves a cloud service provider (SP) establishing the backup infrastructure (hardware and software) and supplying the necessary operational support to keep it running. BaaS solutions can range from simpler "do it yourself" options where the customer provides operational labor to more full-service options where the cloud SP supplies most of the operational manpower. However, the type of solution that is best will vary according to the needs of the IT group.

Among the most important emerging capabilities for BaaS is the ability to protect software-as-a-service (SaaS) applications. SaaS applications (i.e., CRM, ERP, messaging) often do not have adequate data protection that meets corporate data retention, recovery, or other governance mandates. It is important for IT buyers to understand that SaaS applications commonly have a "shared responsibility" model toward data protection. That is, the vendor provides only basic protection, and it is the customer's responsibility to provide any capabilities beyond that as required.

An example of basic data protection SLAs would be daily backup (i.e., recovery point objective [RPO] equal to 23 hours) with 30 days of retention and 10-day recovery time objective (RTO). This is inadequate for many organizations.

Current self-managed approaches to SaaS data protection often lead to operational challenges and suboptimal results, such as delays in data restore or even lost data. Moreover, our research shows that organizations average three different backup software products, while some have as many as seven. The impetus for implementing so many redundant solutions is the need to protect diverse workloads where a single tool is incapable of addressing all requirements. However, multiple backup products increase IT staff labor and introduce inconsistencies of governance policy application. In the face of these challenges, organizational leaders are looking to simplify backup systems and operations that deliver better SLA attainment through consolidated, cloud-based solutions.

Benefits

BaaS offers organizations the opportunity to standardize their data protection operations and policies across core, cloud, and edge. BaaS can relieve IT teams of the need to deploy and manage backup infrastructure by offloading those systems and tasks to a qualified cloud SP. BaaS infrastructure is kept up to date by the provider, meaning that organizations no longer must worry about patch management, software upgrades, component interoperability, or opening vulnerabilities due to out-of-date software. BaaS solutions are almost universally sold as a subscription so that organizations do not have large up-front investments in infrastructure or the risk of orphaned software licenses.

Established BaaS solution providers have the breadth of experience to apply expertise to a variety of scenarios, whereas many IT organizations will have a scope of experience limited primarily to their own environment. Whether the issue arises from an ordinary data loss, a natural disaster, or a cyberattack, providers can bring to bear their experiences from many customers and assist all customers in avoiding common pitfalls. BaaS providers are also likely to have a set of best practices to assist customers in optimizing their experience, which will be cloudlike regardless of repository.

Because BaaS is inherently cloud based, it offers cloud economics, flexibility, and scale. On-demand cloud services match value to price and allow organizations to scale up or scale back according to usage, whether it be seasonality or unpredictable factors. Subscriptions can be short term if needed or longer term to lock in better prices and terms.

BaaS solutions can be coordinated with other data protection products, such as disaster recovery as a service (DRaaS) and archive as a service (AaaS) to gain ever greater leverage on value. Having common functionality between these products provides simplification and greater assurance of data recovery across all potential loss events.

Key Trends

Backup is no longer regarded as a separate IT operation; it is a part of the overall infrastructure and data management strategy. Thus, backup operations are being incorporated into cloud infrastructure and data management platforms with their own policy engines for governance and management consistency. These platforms provide consolidated operations for backups across the enterprise, whether core, cloud, or edge. They also provide a common user experience across operating environments that is cloudlike in its operation.

Cyberattacks are the greatest risks to data integrity and resilience, and they are a concern of both business and technical leaders. Backup operational effectiveness is the baseline for cyber-recovery, but organizations must look holistically at the problem and architect a solution that incorporates cybersecurity with data protection and select products that provide this integration.

Considering HPE GreenLake for Backup and Recovery

Hewlett Packard Enterprise (HPE) has been a major provider of enterprise infrastructure systems and solutions for many decades. Since its spin-off from Hewlett-Packard, the company has focused on servers, storage, and other hardware infrastructure systems. HPE has been building its storage software solutions portfolio and focusing on storage software and data management capabilities.

Introduced in 2021 as a part of HPE GreenLake for data protection, HPE GreenLake for Backup and Recovery is BaaS designed for hybrid cloud. This service simplifies how to protect VMware virtual machines (VMs) running on any storage across hybrid cloud, bringing with it the cloud experience and flexibility of software delivered as a service.

HPE has made enhancements to HPE GreenLake for Backup and Recovery to protect Amazon EBS volumes and EC2 instances with the cloud-native HPE service. The enhanced solution now enables consistent backup and restore of data on premises or in the cloud with a global protection policy. It also eliminates data silos and is delivered on a secure platform with built-in protection from ransomware.

HPE GreenLake for Backup and Recovery is a true SaaS solution protecting on-premises VMs and cloud-native workloads. All operations are driven and managed by the service. It is a single service to back up and recover on-premises VMware VMs, Amazon EBS volumes, and EC2 instances — quickly and in a few simple steps. There are no additional scripts or code to develop, saving time and resources. This service is managed by a single cloud console. Single policy-based orchestration and automation help form custom protection groups. These groups help enforce organizationwide protection policies that define the required recovery SLAs across all protected data types.

HPE GreenLake for Backup and Recovery provides organizations with views into multiple VMs and AWS accounts. An organization can administer backup and recovery for VMs, Amazon EBS volumes, and EC2 instances from a single console. A user can quickly see the dashboard and apply the appropriate protection policies.

This service integrates the HPE StoreOnce Catalyst technology, which provides space-efficient backups enabling HPE GreenLake for Backup and Recovery to deliver optimized backup storage efficiency. HPE GreenLake for Backup and Recovery stores data in a compressed, deduplicated format to help reduce the cost of backup storage capacity and drive down the cost of backup data retention. The service is intended to deliver optimal storage efficiency.

HPE GreenLake for Backup and Recovery encrypts data in transit and at rest with the option of storing backup data in an immutable format. Backup copies are made inaccessible to ransomware to help ensure data backup security. Backup data immutability is key to preventing a backup from being deleted or modified before the configured retention date. Preserving the backup copies is important for any organization's ransomware mitigation strategy.

With additional security features such as dual authorization set, a second approver with the role "Administrator" or "Backup and Recovery Administrator" is required for deletion of a backup or snapshot. Dual authorization is intended to prevent both ransomware attackers and potential internal threats from unilaterally interfering with data backups. HPE GreenLake for Backup and Recovery stores backups outside of the customer's environment, which prevents out-of-band access, ensuring adherence to the defined policies.

HPE GreenLake for Backup and Recovery provides a consumption-based, pay-as-you-go experience and fixed commitment subscriptions while backing up on-premises VMware VMs and cloud-native Amazon EBS volumes and EC2 instances.

Because everything is managed by the service, customers don't have to deal with complex software licensing or manage cloud infrastructure. There are no additional charges for data egress, ingress, or search operations.

This data protection service is delivered through the HPE GreenLake platform as a part of HPE GreenLake cloud services. Users can use cloud data services from HPE GreenLake to orchestrate compute, provision storage resources, and protect workloads with unified access and experience. This solution creates a single, companywide data management approach to break down all data silos with agility and cloud operational experience to help customers eliminate complexity.

Challenges

Backup as a service is a fragmented and highly competitive market with an estimated 4,000–6,000 independent cloud SPs worldwide engaged in providing solutions. Many providers focus on very specific niche markets, either regionally or by industry. HPE can use its breadth of product solutions to compete strongly but will be most effective with customers that have fully adopted other HPE solutions, including HPE GreenLake; HPE will find challenges in competing in specific niche markets.

In addition, HPE must compete with other major cloud BaaS solutions. Several software vendors now offer BaaS directly with their own supporting ecosystems. Moreover, cloud hyperscalers have become more assertive in data protection solutions, all of which makes for a very hard-driving market.

Conclusion

Given the breadth of threats to data integrity today, effective data protection has never been more important or more difficult. SaaS applications introduce a unique opportunity and challenge to IT leaders because while the SaaS provider controls the data, the shared responsibility model of SaaS means the IT organization is responsible for the data. Therefore, SaaS applications and traditional applications require different approaches to protection.

Cloud is emerging as the dominant data protection platform. With most organizations deploying hybrid cloud architectures, using cloud-based data protection — especially BaaS — becomes a natural evolution. Unifying data protection with solutions that offer a cloudlike experience regardless of application platform is the desire of most IT managers.

With most organizations deploying hybrid cloud architectures, using cloud-based data protection — especially BaaS — becomes a natural evolution.

BaaS offers IT teams the ability to offload mundane data protection tasks and free up time for higher-value activities. It also brings to bear the breadth of experience of the provider and the best practices associated with that experience. Solutions such as HPE GreenLake for Backup and Recovery not only provide comprehensive data protection but also fit within a greater data management framework to improve visibility into backup operations and help simplify them.

About the Analyst

Phil Goodwin, *Research Vice President, Infrastructure Systems, Platforms and Technologies Group*

Phil Goodwin is a Research Vice President within IDC's Infrastructure Systems, Platforms, and Technologies Group, with responsibility for IDC's infrastructure software research area. Mr. Goodwin provides detailed insight and analysis on evolving infrastructure software trends, vendor performance, and the impact of new technology adoption.

MESSAGE FROM THE SPONSOR

More About HPE GreenLake for Backup and Recovery

Watch how HPE GreenLake for Backup and Recovery helps to secure on-premises VMs and cloud-native workloads in few simple steps within minutes.

Users can try the service with 90-day free trial and experience the benefits before subscribing.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on https://www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com