IDC TECHNOLOGY SPOTLIGHT

Sponsored by: HPE

Siloed data; data growth; data sprawling across core, cloud, and edge; and increasing ransomware/malware threats have contributed to unprecedented complexity and greater risk of data loss for IT organizations. DPaaS solutions can deliver centralized data protection that simplifies operations and helps defeat ransomware attacks.

Using Data Protection as a Service to Address Modern Data Threats

November 2021

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

Introduction

According to IDC research, 55% of organizations will have implemented a cloud-centric data protection strategy by 2025. This means that organizations will implement and manage their data protection in the cloud, even for workloads that remain in the core or that may be deployed at the edge.

Drivers of this change include data growth, which our research indicates is increasing at a 43% compound annual growth rate (CAGR) for large-scale organizations. This means that data volumes double roughly every three years. Although 50% of data remains in the core, data is growing faster in the cloud and at the edge. Application deployments are also driving this change. We forecast that 80% of new application deployments will be in the cloud or at the edge. As the preponderance of data and applications moves toward the cloud, so will the data protection strategies to protect them.

AT A GLANCE

WHAT'S IMPORTANT

IDC forecasts that by 2025, 55% of organizations will have implemented a cloud-centric data protection strategy.

KEY TAKEAWAYS

Data protection as a service (DPaaS), including backup as a service (BaaS), disaster recovery as a service (DRaaS), and archive as a service (AaaS), offers the agility, flexibility, and enterprise breadth to help organizations modernize and improve data protection operations.

This move to the cloud and edge has created a serious challenge for IT organizations: data silos. Data may become siloed because of location, data type, data owner, and many other factors. IDC research, sponsored by Zerto, a Hewlett Packard Enterprise (HPE) company, and conducted worldwide, found that companies commonly deal with 14–20 different silos. Siloed data leads to labor inefficiencies, inconsistent data management and governance policies, redundant and costly toolsets, and greater risk of attacks on data and data loss. These silos also stymie an organization's ability to effectively leverage data because of the data management barriers between silos.

The same IDC research showed that 91% of organizations have experienced a technology-related business disruption in the past two years; 84% have been attacked by malware or ransomware in the past two years; and 56% have experienced an unrecoverable data event within the past three years. These statistics are alarming and illustrate the need for modern data protection solutions to address the increasing and evolving threats. With data availability at the core of data value, organizations must mitigate these threats and challenges.

Data protection as a service (DPaaS) solutions have emerged as cloud-centric strategies to tackle the changing nature of data protection. According to IDC research, DPaaS is the fastest-growing segment of the data protection market with a forecast 19.1% CAGR through 2025. DPaaS includes backup as a service (BaaS), disaster recovery as a service (DRaaS), and archive as a service (AaaS). DPaaS solutions are not just for cloud repositories; they can meet on-premises and edge data protection requirements as well. IT organizations that adopt DPaaS solutions can simplify operation and infrastructure management, apply consistent data management policies across the enterprise, and deal with rising ransomware recovery needs.

Definitions

- **Service provider (SP).** An organization that delivers as-a-service solutions, usually maintaining the infrastructure (hardware, operations software, and solutions software) at minimum within a public cloud environment (Service providers may offer a range of solutions from "do it yourself" infrastructure where the customers take on a great deal of the effort to "white glove" full-service solutions that outsource the effort to the SP. Service providers include cloud SPs and managed SPs.)
- **Backup as a service.** Cloud-based infrastructure (compute and storage) and data movers (i.e., backup/recovery software) to move data from a source location (on premises, cloud, or edge) to a public cloud repository as a backup data set
- **DR as a service.** All the functionality of BaaS plus the infrastructure (compute, storage, network, authentication, etc.) and processes needed to restore a workload to business-level operations in a public cloud environment
- **Archive as a service.** Public cloud infrastructure, including data movers, to low-cost storage with a low expectation of data access and potentially low service levels

Benefits

DPaaS solution providers can relieve organizations of mundane tasks related to infrastructure management, backup, DR, and archiving and thus free up resources for higher-value tasks. DPaaS services can consolidate operations for on-premises, cloud, and edge data protection, all with management from the central cloud service. Service providers are responsible for managing, maintaining, and updating the infrastructure, again relieving IT of these common tasks. Some SPs offer "hands and feet" services to bring systems back online or manage recovery and testing operations as a supplement to the IT team. During an actual data recovery emergency, the SP's staff may be able to facilitate the recovery when the primary IT staff is unavailable.

DPaaS solutions offer greater flexibility and deployment options with consumption-based subscriptions to match costs, providing value with easy scale-up/scale-down options. With DRaaS in particular, the as-a-service solution significantly reduces the cost of DR compared with the cost of traditional site-to-site recovery of on-premises solutions. When DPaaS encompasses on-premises data protection requirements, such as local backup repositories and purpose-built backup appliances, DPaaS recovery orchestration can determine the fastest restore path, thereby reducing unplanned downtime and data unavailability.

Because the hardware infrastructure and software systems are already installed and operational for DPaaS solutions, IT organizations can implement DPaaS solutions more quickly and more easily than on-premises solutions. Much of the effort by the IT group will be devoted to establishing data management policies and backup schedules rather than just getting systems up and running.

Testing has long been a major challenge for DR systems and one that too often is overlooked or delayed by IT teams. Recovery and DR testing in the cloud for DRaaS can utilize the flexibility of the cloud to deploy resources and conduct nondisruptive testing. As a result, testing can be conducted more frequently to increase an organization's confidence in the preparedness of data recovery and facilitate faster and more certain recoveries in the event of an actual failover.

Cloud-based solutions can often leverage immutable storage to preserve copies needed for ransomware recoveries. These immutable repositories ensure data integrity and reduce the chances that an organization would need to pay a ransom. In addition, automated tiering can move data from on premises or the edge to the cloud and into this immutable storage.

It is also important that organizational leaders understand that software-as-a-service (SaaS) solutions should not be overlooked for data protection needs. Data protection schemes for individual applications are often minimal with low-requirement service-level agreements (SLAs), neither of which may meet corporate requirements. DPaaS solutions can be deployed to automate cloud-based data protection for SaaS applications and ensure proper data retention and other governance compliance.

Trends

Data is increasingly moving to the cloud and edge. Recent IDC research shows that 50% of data is in the core, 22% is in the cloud, 19 % is at the edge, and 9% is in "other" locations. As data in the cloud and at the edge is growing faster than data in the core, as noted previously, organizations will find it more convenient and operationally practical to manage data protection from the cloud.

Data protection solutions are also evolving past standalone backup and recovery applications. Higher-level data management functionality is including data protection along with data security and data logistics. In response, data management platforms are emerging to meet these broader needs and becoming more high profile in their ability to deliver the data availability and reliability required by modern data-driven organizations. Pervasive ransomware and its consequences have elevated the need for DR responses and assured recovery, two features that are now part of data management platforms.

Among the most interesting and important enhancements to data protection are artificial intelligence (AI) and machine learning (ML), both of which are growing in capabilities. AI and ML will be key to automating and simplifying operations, such as resource planning, optimization, fault recovery, performance, and SLA attainment. In addition, AI is playing an important role in detecting and mitigating malware and ransomware by identifying anomalous data activity and alerting administrators or initiating defensive action. The complexity of IT systems is growing such that intelligent automation will be required for IT teams to stay abreast of data management and threat mitigation.

Considering HPE

Hewlett Packard Enterprise has been a major provider of enterprise infrastructure systems and solutions for many decades. Since its spin-off from Hewlett-Packard, HPE has focused on servers, storage, and other hardware infrastructure systems. Recently, the company has pivoted to building its storage software solutions portfolio and focusing on storage software and data management capabilities. In mid-2021, the company acquired Zerto, an organization known for its disaster recovery and ransomware recovery and workload migration solutions.

As part of the transformation of HPE storage into a cloud-native data services business, HPE has entered the rapidly growing DPaaS market with HPE GreenLake for data protection. It offers what it positions as the next generation of data protection cloud services: disaster recovery service with Zerto and backup with HPE Backup and Recovery Service. These new services offer customers the flexibility to modernize data protection — from rapid recovery to ransomware protection to long-term data retention — either on premises or in the public cloud with operational simplicity. Together, these innovations further accelerate HPE's transition to a cloud services company with the intent of giving customers greater choice and freedom for their business and IT strategy, with an open platform that provides a cloud experience regardless of location. The new offerings, which add to a growing portfolio of HPE GreenLake cloud services, allow customers to innovate with agility, manage costs, and secure data from the edge to the cloud and address ransomware attacks and other cyberattacks.

Following the close of the Zerto acquisition, HPE has added Zerto's data protection to its cloud services portfolio to help enterprises address cyberthreats and ransomware attacks. Zerto's Continuous Data Protection (CDP) technology with journal-based recovery helps customers recover from an attack in minutes and restores data to the state it was in just seconds before the attack occurred. With Zerto's ability to migrate data and workloads to and from the cloud, backup and DR are enabled for on-premises workloads, cloud-native workloads (including containers), and SaaS workloads. This ability to migrate between cloud and on premises gives customers the flexibility to optimize recovery solutions.

In addition, HPE GreenLake for data protection includes the recently announced HPE Backup and Recovery Service for VMware workloads. It is backup as a service designed for hybrid cloud. Delivered through a SaaS console with policy-based orchestration and automation, HPE claims that virtual machines (VMs) can be protected with three simple steps and in less than five minutes. Backup management is facilitated across on-premises and hybrid cloud through a single cloud console. Managing this service does not require additional media servers, appliances, or data targets. Customers can recover rapidly on premises, benefit from the cost effectiveness of long-term retention in the public cloud, and have the security of backups that are protected against ransomware attacks. The solution offers consumption-based pricing with data reduction technologies such as deduplication and compression to reduce total costs.

With HPE GreenLake for data protection, customers can secure their data against ransomware, recover from any disruption, and protect their VM workloads across on-premises and hybrid cloud environments. HPE is working to make data protection as simple as configuring recovery point objectives (RPOs) and recovery time objectives (RTOs).
Using these policies, customers can apply the right blend of disaster recovery, backups, and archive technologies, all of which are auto-configured and auto-managed for protecting data and applications across on-premises, hybrid cloud, and multicloud environments.

Challenges

Although the DPaaS market is growing rapidly, it is also a very crowded space with thousands of service providers worldwide offering solutions. Thus, HPE is moving into an established market at a time when many other organizations are already offering competing solutions. However, the HPE brand stature will allow the company to gain immediate recognition and credibility.

The complexity of today's application environments also means that it is nearly impossible to address every requirement, challenging HPE development resources to keep up with requirements and prudently choose which use cases HPE intends to pursue. Although the combination of HPE and Zerto appears to be very complementary, there are many technical details to work out on the integration, which may either delay or stymie specific capabilities. HPE and Zerto have stated that they are working toward integrating these services soon.

Conclusion

DPaaS solutions for backup, DR, and archiving have gained rapid adoption in the marketplace. The flexibility of cloud solutions, including deployment alternatives, on-demand resources, consumption-based pricing, and other factors, makes DPaaS very compelling to many IT buyers. Rather than having to purchase, install, configure, manage, and maintain backup infrastructure, organizations can turn these tasks over to service providers. As a result, IT teams not only spend less time on labor and training but also avoid many day-to-day headaches.

DPaaS solutions for backup, disaster recovery, and archiving have gained rapid adoption in the marketplace.

As data protection, recovery, and DR rise in importance in the face of growing cyberthreats and the increasing data needs of data-driven organizations, IT teams are turning not only to DPaaS but also to data management platforms that integrate many aspects of data logistics, data security, and data use. These platforms help break down data silos by providing an enterprise perspective to data governance, data security, cyber-recovery, and service-level attainment.

The combination of HPE GreenLake, HPE Backup and Recovery Service, and Zerto brings together crucial components of data management across the core, cloud, and edge with a cloud-like experience regardless of where the data resides. HPE's pivot to data management software puts the company at the forefront of this trend with a rapidly growing portfolio of solutions. The acquisition of Zerto brings a proven DR, ransomware recovery, and backup solution to the growing HPE GreenLake ecosystem. With the addition of this solution, plus existing backup capabilities and HPE's status in the IT market, HPE is well-positioned to gain rapid traction in the fastest-growing segment of the data protection market: DPaaS.

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. His focus is on multi-cloud data management, data logistics, on-premises and cloud-based data protection as a service, cyber protection and recovery, recovery orchestration, and more.

MESSAGE FROM THE SPONSOR

About HPE

Learn more about HPE's latest offerings:

https://www.hpe.com/us/en/greenlake/data-protection.html

https://www.youtube.com/watch?v=5ZJXXpwm1Rw

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on 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

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.