SPOTLIGHT

Sponsored by: Commvault and AWS

"Data everywhere," ransomware, and the speed and scale of modern business, all challenge IT teams to assure data resilience. Leveraging cloud resources for data protection can improve a company's risk profile, lend agility, and lower the cost of operations.

Improving Data Resilience with a Cloud-First Approach

January 2024

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

Introduction

Modern ITOps teams have an unenviable task. Data is the most valuable resource for many organizations, so making sure that it is available, accurate, and timely is a nonstop effort. To make things even more difficult, ITOps and SecOps teams — which have not historically worked closely together — must now coordinate efforts to assure preparedness against ransomware. Organizations need a proactive stance toward cyber-resilience. However, IT leaders know that no amount of preparation is guaranteed to keep attackers out. Therefore, having absolute certainty of data survival and recovery in the face of any attack type is a requirement for any organization. Even so, the ITOps team cannot lose sight of the daily operational tasks needed to assure data survival against any threat.

AT A GLANCE

WHAT'S IMPORTANT

Data proliferation, data silos, and ransomware can lead to serious business risks and runaway costs.

KEY TAKEAWAY

Cloud computing has fundamentally changed the convenience, capabilities, and economics of data protection. Whether operated by the ITOps team or as a service by a cloud provider, cloud services offer important functions with the cost optimization of on-demand services.

It is cliché to say that data volumes are at never-before-seen levels, because that has been the case almost every year since the advent of computing. Unfortunately, this trend is going to continue to be true for years to come. IDC predicts the total amount of commercial data stored will be 12.8ZB by 2026 (see IDC's *Worldwide Global DataSphere and Global StorageSphere Structured and Unstructured Data Forecast,* 2022–2026, IDC #US49084022, May 2022).

These massive amounts of data are spread across organizations in dynamic application workflows. Our research shows approximately 49% of data is in the traditional datacenter, 29% is in the cloud, 19% is at the edge, and 4% is located elsewhere. However, the trend is from the datacenter toward the cloud and edge. This data may also be segregated by platform (i.e., physical Windows, virtual infrastructure, Linux, Unix, and other legacy platforms), structured data, unstructured data, NoSQL data, and containerized environments. This combination of factors or any one of them often causes data to become "siloed." When data becomes siloed, each silo may entail different storage and protection policies as well as redundant data management and backup products along with the duplication of training and labor needed to manage them. Worse yet, the silos open more points of vulnerability as cyberattacks become sophisticated with generative AI. The bottom line is greater risk, higher costs, and more labor.

To deal with these factors, IT leaders are looking for better ways to streamline operations while improving data availability, reducing risk, and avoiding costly budget increases. Cloud computing and data protection as a service can improve data availability operations in all these aspects.

Definition

- **Data availability:** Data is not only available for access but also accurate and complete. Data availability can be measured in system uptime that gives a user or an application access to data as well as in data loss; that is, lost data obviously is unavailable. Said differently, data availability is hampered by downtime and unrecoverable data. Data availability should not be confused with high availability (HA), which is a hardware configuration designed to recover from system faults. HA may be a means to enhance data availability but is a different technology.

Options and Benefits

Cloud-based data protection is a key use case for cloud computing. Cloud offers scale, economics, and flexibility that may not be attainable on premises. The principal methods of leveraging the cloud for data protection include:

- **Cloud as a target or tier**. Whether data resides on premises or in the cloud, ITOps teams may use the cloud as a backup target, either as the primary target or as a second "tier." Using this method, backup software manages the data movement and backup catalog, regardless of data location. A key benefit of using the cloud is fulfilling the requirement to have an offsite data copy for disaster recovery (DR) or other survival purposes. Organizations may also choose to move or copy the data to additional cloud data zones for added safety. Cloud as a target or tier is usually self-managed by the ITOps team.

- **Backup as a service (BaaS).** BaaS is normally handled by a third-party provider managing backups from the cloud and storing the data in the cloud, whether primary data resides on premises or in the cloud. Data is restored from the cloud to the original location. The primary benefit of BaaS is offloading management of the backup environment to a third party, which frees the ITOps team to address high-priority tasks. BaaS options range from basic infrastructure services to "white glove" fully managed plans.

- **Disaster recovery as a service (DRaaS).** Traditional DR required redundant datacenters and equipment, all at considerable cost. DRaaS fundamentally changes the economics of DR to make it affordable regardless of organizational size. DRaaS providers establish the necessary failover infrastructure in the cloud and data storage needed to recover applications if the primary site fails. Organizations can choose from standby infrastructure to on demand, depending upon recovery time requirements and budget constraints. As with BaaS, DRaaS offerings range from DIY to white glove to either supplement the ITOps team or offload DR to the provider entirely.

- **Cyber-recovery as a service (CRaaS).** CRaaS is an emerging category of service that builds on BaaS and DRaaS to add the necessary components needed for cyber-recovery. This includes such things as isolated "clean rooms" for forensic analysis, malware scanning, and removal tools. CRaaS providers may also be able to provide added services such as risk posture management, incident response teams, and crisis communications. CRaaS providers can offer expertise not common in ITOps teams to provide faster, more certain recovery from cyberattack.

- **Archive as a service (AaaS)**. AaaS is similar to BaaS in that the cloud is used as a target for archive data sets. AaaS providers often leverage the lost-cost archive storage tier in the cloud to minimize cost. As with other as-a-service solutions, AaaS relieves the IT organization of mundane archive tasks.

Cloud solutions typically have different classes of storage services to satisfy different data protection (and other application) needs. For example, production-grade storage may be accessed on demand for disaster recovery scenarios, low-cost archive storage may be used for archive, and immutable storage may be used for cyberprotection.

Workload agility is another key use case for cloud computing. Because applications require different storage types, cloud offers the ease of accessing the right type without having to purchase and manage specialized storage arrays for each. Cloud storage can be optimized for structured or unstructured workloads, containerized workloads, and cloud-native workloads.

Considering Commvault and AWS

Commvault and AWS have collaborated to bring customers joint solutions, whereby Commvault provides cyber-resilience that leverages AWS for secure and scalable cloud data storage and compute resources. Each vendor is discussed in the sections that follow.

Considering Commvault

Commvault offers comprehensive cyber-resilience and data security solutions for on-premises and cloud-based workloads. The company utilizes backup to the cloud, either from on premises or within the cloud. The Commvault Cloud platform includes backup and recovery, proactive cyberdefense, forensics, governance, threat detection, monitoring, and reporting. Commvault also offers a BaaS solution with a data plane that runs on Amazon EC2 and utilizes Amazon S3 and Amazon S3 Glacier as storage targets.

Commvault protects workloads running in AWS such as Amazon EC2, Amazon EBS, Amazon RDS, Amazon Aurora, Amazon Redshift, Amazon FSx, Amazon S3, and more, as well as leveraging storage services like Amazon S3 and Amazon S3 Glacier as a backup target. Commvault also has ways to optimize customers' cloud costs through deduplication and compression of stored backup data, elastic resource provisioning, and integration points that accelerate how data is accessed and recovered through native AWS APIs. Commvault can also automate the recovery and migration of workloads to AWS to provide on-demand disaster recovery and accelerate adoption of new cloud services.

Considering AWS

AWS is a major cloud provider, offering a wide range of services. With datacenters around the world, AWS can offer services and tools for application failover and data replication to numerous geographical locations to optimize protection, performance, and uptime. Storage services offered by AWS include:

- **Amazon S3:** Secure, durable, and scalable object storage
- **Amazon EFS:** Shared storage for file services
- **Amazon S3 Glacier:** Low-cost, secure, and durable storage for archive and backup
- **Amazon FSx:** Launch, run, and scale a high-performance and widely used file systems: NetApp ONTAP, OpenZFS, Windows File Server, and Lustre in a few clicks

Challenges

Data protection is a highly dynamic market with many different permutations of systems, services, and requirements. Although Commvault and AWS are among the largest in their respective markets, no vendor of any size can satisfy every customer requirement. Moreover, in collaboration with companies such as Commvault and AWS, the companies' development processes are independent of one another and may or may not sync up on any specific release or capability. While the two endeavor to meet their mutual customer's needs, there may be times when companies will need to wait on one for the support of the other.

It is also important for customers to understand that simply backing up to the cloud does not satisfy air-gapped requirements for cyberprotection purposes. Additional steps must be taken to separate the data plane from the control plane for cloud storage to minimize the opportunity for attackers to compromise both on-premises and cloud backups. IT organizations will also need to use services such as Amazon S3 Object Locking to achieve immutability. IDC recommends cloud storage, including immutability options, as important components in cyberprotection strategies; these repositories can provide valuable protection. IT teams should use a layered approach to protection schemes that utilize other capabilities to assure data survival and integrity.

Conclusion

As organizations seek to improve their data resilience posture, the majority are implementing centralized data resilience solutions with the scale, flexibility, and economics of the cloud. By combining advanced cyber-resilience software and operations with cloud resources for storage and immutability, IT teams can take proactive measures to minimize the chances of a debilitating ransomware event. Fast, certain, and accurate data recovery can give business and IT leaders alike confidence in recovery without paying a ransom. With these cloud resources and advanced software solutions, organizations can implement layered protection strategies that give it the best opportunity for fast, accurate recovery from cyberattack. As-a-service solutions, whether for backup, disaster recovery, or cyber-recovery, simplify those operations and leave the IT team time to pursue higher-value projects.

About the Analyst

Phil Goodwin, *Research Vice President, IDC's 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 multicloud data management, data logistics, on-premises and cloud-based data protection as a service, cyberprotection and recovery, recovery orchestration, and more.

MESSAGE FROM THE SPONSOR

For more information about how Commvault and AWS are working together to solve their customers' most difficult challenges relating to cyber resilience and data security, visit commvault.com/aws.

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