IDC

ANALYST CONNECTION

Sponsored by: Google

The need for accurate, available data has never been greater. Yet, the threats to that data have never been more intense. Cloud-based data protection and cyber-recovery can deliver the data availability organizations need with flexibility, agility, and lower TCO.

The Data Protection Imperative for Cloud Workloads

October 2022

Questions posed by: Google

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

Q. Why is it important for companies to have a backup and disaster recovery (DR) strategy for their cloud workloads, and what are the key components of such a strategy?

A. At the most fundamental level, backup is the foundational component of data availability, data resilience and, in many cases, digital transformation. Without rock-solid backup, none of these things are possible. Disaster recovery uses backup as an essential component in the overall strategy, but whereas backup is focused on data, DR addresses the entire application stack. Indeed, organizations need application availability, not just data availability.

Cloud workloads can be deployed in several ways. The most basic deployment is a refactored workload — in other words, moved from on premises to the public cloud. In these cases, the entire stack must be addressed in the migration, such as the underlying database for apps such as SAP. A "cloud-native" deployment often involves container-based workloads, although containerization is not required. These "born in the cloud" applications are architected specifically to take advantage of cloud capabilities, such as different classes of storage, functionality such as immutability, and so on. In a software-as-a-service (SaaS) deployment, the application is offered and supported by a third party based on a subscription model. Examples are Google Workspace and Salesforce.

Regardless of deployment type, data protection is a "shared responsibility" model where basic availability is provided by the cloud or service provider, but the customer is responsible for data protection activities, data governance, and DR. Data backup of cloud workloads, as with on premises, is foundational to data availability and is a requirement for cloud workloads. Data replication from zone to zone or region to region can help ensure availability or data survival in the event of an issue at the primary cloud datacenter. Immutable cloud repositories can also help ensure data survival from accidental deletion or intentional attack. Archive tiers in the cloud satisfy long-term retention and governance requirements.

Q. How does a cloud-based backup strategy help with ransomware recovery?

A. Cloud can play an essential role in cyber-recovery (CR), whether the workload is on premises or in the cloud. For example, immutable cloud repositories and properly configured air-gapped copies provide offsite data storage that ensures data survival for on-premises data. That data can be further replicated to other zones or regions for even greater safety of all data. These capabilities are key to protecting and recovering data from a ransomware attack.

The on-demand nature of cloud is well suited to DR, which extends to cyber-recovery because many DR components are foundational to CR. Because DR and CR utilize common infrastructure, organizations can often use the same provisioned components. However, CR has additional requirements, such as a secure, fenced-off sandbox for forensic analysis and recovery testing.

IDC predicts that 55% of organizations will adopt a cloud-centric data protection strategy by 2025. This means that the protection for workloads across the organization will be managed through cloud-based data protection products and services, including basic backup, archive, DR and CR, and cloud-native solutions from cloud providers. IDC further forecasts the CR market to reach $317.7 million by 2026 (149% CAGR).

Q. How should companies approach backup, disaster recovery, and cyber-recovery as they extend their operations to the cloud? For example, how should budgets change?

A. Cloud economics have fundamentally changed DR deployments. When DR involved redundant datacenters and infrastructure, many organizations chose to take the risk of outage rather than spend the money. Organizations outside of natural disaster zones, in particular, viewed DR as expensive "insurance."

Cloud changed all that. With cloud, organizations can take advantage of on-demand resources to avoid costly datacenter duplication and engage with disaster recovery as-a-service (DRaaS) providers that can help with setup, testing, and recoveries. Moreover, the cloud provider manages the infrastructure. The provider ensures that the systems are up to date and working, and if something goes wrong, the provider takes care of it. This frees up the IT staff to attend to other activities.

When it comes to ransomware, everyone is in a ransomware zone. Our research shows that nearly half of organizations have been successfully attacked within the past three years and less than a third of those were able to fully recover without paying the ransom. This poor result would indicate that many organizations are not adequately prepared for a ransomware attack. Every organization needs a ransomware strategy and a plan to recover.

While implementing a cyber-recovery plan costs money, it is usually easily justified by offsetting cost avoidance. Our research shows that ransomware attacks can be costly to recover from (including the ransom) in terms of lost revenue, lost employee productivity, and permanently lost customers. Moreover, as more organizations purchase ransomware insurance, having a solid, demonstrable plan can help them qualify for lower premiums. In many respects, organizations simply cannot afford to not invest in robust cyber-recovery measures.

Q. What are the top advantages that cloud providers can offer customers for backup, DR, and CR today and in the future (i.e., by leveraging some of the inherent cloud capabilities)?

A. Cloud-based data protection — whether backup, DR, or CR — offers a number of important capabilities. The first is on-demand systems that can be quickly, easily, and economically deployed and scaled. Second, whether the data protection is a DIY effort or using a service provider, cloud can be used to meet best practices such as immutability, encryption, and data copies across multiple physical locations. And third, the cloud hyperscaler may offer data protection services within its cloud platform to offer native cloud data protection. Cloud implementations are often based on standardized configurations established by the cloud provider based on best practices that facilitate faster time to production with less management effort. Cloud reporting facilities provide better visibility into infrastructure, data, operations, and service-level management.

Along the same lines, cloud provider partnerships with cyberinsurance providers can enable organizations to more easily demonstrate their cyberprotection preparedness, thereby leading to lower premiums. Further, the broad scope of cloud provider solutions, including data protection capabilities for both on-premises and in-cloud workloads, provides an opportunity for customers to leverage cloud-native solutions to simplify DR and CR workflows.

Q. What are some capabilities and solutions that cloud providers can offer to customers to meet their RPO/RTO requirements while optimizing for costs, especially given the continued growth in data?

A. Data protection should be viewed as a continuum of capabilities. Backup and recovery is the foundational element, as mentioned previously, and archive builds upon backup and recovery; disaster recovery likewise builds on backup and recovery, and cyber-recovery builds on disaster recovery. Cloud resources for these capabilities can be multipurposed to provide better data resilience at a low incremental cost and a high degree of resource leverage.

Data protection services in the cloud offer IT organizations a wide range of options, from simple DIY implementations to "white glove" options that deliver a high degree of professional services. IT buyers can select solutions based on their particular requirements and organizational skill sets. Services selections can also be made based on RPO, RTO, and levels of resilience offered by the provider. Services can also be scaled up or down based on seasonality, data growth, and other criteria to optimize TCO versus service level. The bottom line is that cloud-based data protection offers broad flexibility and capabilities so that organizations can pay for exactly what they need, reduce the IT workload, and deliver the services required by the business.

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 multicloud data management, data logistics, on-premises and cloud-based data protection as a service, cyber-protection and cyber-recovery, recovery orchestration, and more. Mr. Goodwin takes a holistic view of these markets and covers risk analysis, service-level requirements, and cost/benefit calculations in his research.

MESSAGE FROM THE SPONSOR

Google Cloud offers managed backup and disaster recovery (DR) service for centralized, application-consistent data protection

As this report presents, backup is a fundamental aspect of application protection, and choosing to work with a cloud provider to protect your data can offer many benefits. Whether the need to restore data is triggered by a user error, malicious activity, or some other reason, the ability to execute reliable, fast recovery from backups is a critical aspect of a resilient infrastructure. Google recently launched Google Cloud Backup and DR Service, which enables businesses to protect workloads running in Google Cloud and on-premises by backing them up to Google Cloud. This service is designed to help you minimize costs and recovery times. Learn more at cloud.google.com/backup-disaster-recovery.

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494
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.