IDC
Analyze the Future

A N A L Y S T C O N N E C T I O N

Phil Goodwin
Research Director, Storage Systems and Software

The Cloud Is Changing Data Backup: Here's What IT Leaders Need to Know

November 2017

Companies are moving applications to the cloud with software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS) usage increasing at a steady rate. IDC research has found that over half of organizations currently utilize a hybrid cloud configuration. For many companies, backing up data to the cloud is the easiest way to begin using the cloud. To achieve the benefits of backup to the cloud without taking on extra risk, IT leaders need to understand the nuances of cloud-based storage services and plan accordingly.

The following questions were posed by NetApp to Phil Goodwin, research director within IDC's Storage Systems and Software research practice, on behalf of NetApp's customers.

Q. How is the cloud changing IT responsibilities for backup and recovery of enterprise data?

A. There's no question that IT organizations are still responsible for protecting and recovering all enterprise data. What makes it more complicated is that applications are now distributed, whether they're on-premises or off-premises. Sometimes they're under IT's direct control, and sometimes they're not. This has implications for organizations in terms of people, process, and technology.

For people, the organization really needs new skill sets that can span the full spectrum of repositories and applications. For process, they need service-level agreement (SLA) consistency and ways to recover and have business continuity across the organization, regardless of application deployment.

For technology, they need infrastructure that will provide the kinds of service levels that are required, regardless of what the application deployment model looks like.

Q. Do SaaS applications such as Office 365 and Salesforce provide the same level of data protection as an on-premises enterprise datacenter?

A. There's a common misperception that SaaS application providers offer the same level of data protection and recovery as IT departments are accustomed to providing within their own organizations. In many cases, the SLAs provided by the SaaS vendor are limited to 30 days of data retention and recovery windows that can be as long as six weeks — and very expensive.

Some examples are accidental deletions that may be unrecoverable after a 30-day period, such as with Office 365, or there may be slow recoveries of folders because a recovery required by the SaaS vendor is all or nothing and does not have the granular ability to address files, folders, or individual portions of data.

Q. How can companies ensure that their SaaS data is adequately protected against common data loss scenarios such as accidental deletions, malware, and ransomware?

A. The first thing any IT organization should do is verify what service levels are available from and provided by its SaaS vendor. The variation between vendors can be considerable.

In the event there is a gap with respect to the service level provided by the SaaS vendor and what's required by the organization, there may be opportunities to use third-party services or products to back up data from the cloud to on-premises or from cloud to cloud. One thing that's very important to note here is that all of this is subject to SaaS vendor policies and capabilities.

Q. What cloud options are available for backing up traditional on-premises applications and workloads, and do they offer advantages versus tried-and-true backup methods, such as disk to disk and disk to disk to tape?

A. The cloud options available include backup as a service, or BaaS, where data is backed up from a traditional on-premises environment into the cloud so that the cloud then becomes a data target for that backup operation.

Other organizations may use cloud gateways that allow them to back up from local infrastructure to similar infrastructure in the cloud, which gives organizations the advantage of being able to leverage existing infrastructure capabilities as well as the knowledge that people have about those environments.

But in many ways, that continues to be very similar to a disk-to-disk type of backup, again to the advantage of the IT organization's current processes. Cloud storage should really be considered for offsite copies based on cost comparisons as well as the opportunity to recover or protect that data in an offsite cloud environment.

Q. When companies back up data to the cloud, how should they protect against vendor lock-in?

A. Vendor lock-in is possible with respect to having data that can be very expensive to remove from a particular cloud vendor. Therefore, we recommend that IT organizations look for opportunities to replicate in what we call a multicloud environment. In other words, replicate from one cloud provider to another cloud provider.

This process may be done through gateway capabilities. It may involve using both cloud vendors as targets, or there may be other variation on that process. But IT organizations need to look for solutions that offer a choice of cloud capabilities, especially if they need to use in-country services to comply with data sovereignty requirements.

We believe that IT organizations will also want best-in-class capabilities around moving data around a cloud-to-cloud environment, whether from private cloud to public cloud or from public cloud to public cloud. The solution requires all types of capability.

ABOUT THIS ANALYST

Phil Goodwin is a research director within IDC's Storage Systems and Software research practice. He provides detailed insight and analysis on evolving industry trends, vendor performance, and the impact of new technology adoption. Mr. Goodwin is responsible for producing and delivering timely, in-depth market research with a specific focus on data protection, business continuity and disaster recovery, and data availability. Mr. Goodwin takes a holistic view of these markets and covers risk analysis, service-level requirements, and cost/benefit calculations in his research.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com