gamechanger Game changing technology for cloud adoption

A step-by-step guide to cloud adoption and data protection

By Brien M. Posey

It is no longer enough to simply hire a cloud vendor and assume that cloud migration will go smoothly.

Today's public clouds are complex, and it is no longer enough to simply hire a cloud vendor and assume that the cloud migration will go smoothly. The best way to ensure a smooth migration is to adopt a step-by-step process for adopting the cloud as a part of your data-protection strategy.

STEP 1: WHY ADD CLOUD SERVICES TO YOUR DATA-PROTECTION STRATEGY?

The first step in adopting the cloud as a part of your data protection strategy is to consider what you are hoping to gain by leveraging the public cloud. While it is true that public cloud use has rapidly gained popularity among IT professionals, it is not prudent to adopt a solution just because it is popular. Taking the time to define your motivation for adopting the cloud as a part of your data-protection strategy can help you stay focused on finding a solution that will achieve the desired results.

For many organizations, the primary reason for adopting cloud services as part of an overall data-protection strategy is financial. Cloud providers, and in some instances even the IT industry, have done a good job of marketing the cloud as being the inexpensive alternative to operating on-premises. The cloud may or may not be less expensive than operating on-premises, depending on the provider's pricing structure and your usage. What the cloud does do is shift expenses from CapEx to OpEx.

In other cases, organizations decide to adopt the cloud because it allows backups to be stored outside of the datacenter, which is important for data survivability. Some organizations take things a step further and adopt the cloud in hopes of being able to use it as a secondary datacenter that can continue to run mission-critical workloads if the primary datacenter goes offline.

Regardless of the motivation to use cloud services, it is important to consider whether you are happy with your existing backup software. If your backup software is problematic, then extending your backup strategy to include the cloud will not address those problems. In such situations, you may need to consider replacing your backup software as a part of your cloud adoption.

STEP 2: WHICH TYPE OF CLOUD SHOULD YOU USE?

The second question that needs to be answered is: Which type of cloud will best allow you to reach your data protection goals? There are several cloud backup

Photoroyalty / Shutterstock.com

options, and not every cloud data-protection mechanism is well suited to an organization's unique needs, so it is important to weigh your options carefully.

Begin by considering what it is that you need to protect. Are you protecting data that resides solely on-premises, or do you also have data in the cloud that needs to be protected? If you do have cloud-based data, then that data will need to be protected just like you protect your on-premises data. For example, you can't stop backing up your Exchange Server data just because you have moved all your users to Office 365. An organization's data protection, retention and compliance requirements do not change just because data has been moved to the cloud.

One of the options that is available for cloud-based data protection is cloud storage, or Storage as a Service, as it is often called. As its name implies, cloud storage allows backup data to be stored within the public cloud. Cloud storage can be used in a variety of ways, but in many cases an organization will configure a cloud storage gateway to act as a backup target. The cloud storage gateway commonly contains storage of its own, which can be used for short-term data protection. However, all the data that is written to the cloud storage gateway is eventually replicated to the cloud.

Another option is to use Backup as a Service (BaaS). BaaS can vary in scope, but usually refers to a cloud provider that acts as a backup provider. In other words,

Taking the time to define your motivation for adopting the cloud as a part of your data-protection strategy can help you stay focused on finding a solution that will achieve the desired results.

backup jobs are executed from a cloud-based backup server, rather than from a local backup server.

Another option that has become quite popular is Disaster Recovery as a Service (DRaaS). DRaaS is like BaaS, but offers the added advantage of allowing workloads to failover to the cloud, where they can continue running. Hence, DRaaS is about providing business continuity.

STEP 3: HOW DO YOU ENSURE SECURITY IN THE CLOUD?

Perhaps the most pressing question for those who are considering adopting the cloud as a part of their data protection strategy, is how to ensure the security of the data, and continued compliance with any applicable regulations. Ironically, even though security and compliance concerns are often cited as being the

Perhaps the most pressing question for those who are considering adopting the cloud as a part of their data protection strategy, is how to ensure the security of the data, and continued compliance with any applicable regulations.

biggest obstacles to cloud adoption, those who have already incorporated the cloud into their data protection solution often find that using the cloud improves security.

There are two primary ways the cloud can help improve data protection security. First, depending on the backup solution that you are currently using, your data may or may not be encrypted. Cloud providers, on the other hand, almost always encrypt data both at rest and in-flight.

The other way the cloud can improve the security of your backups is by restricting physical access. If backups are being performed solely on-premises, then someone with bad intent could conceivably gain physical access to your backup server. For those organizations that create tape-based backups, it may be relatively easy for someone to steal a backup tape containing your most sensitive data.

The cloud provides a layer of physical isolation between your datacenter and your backups. Although this isolation is most commonly discussed from a data survivability standpoint, it also enhances security by making it impossible for someone to break into your datacenter and steal your backup media.

VEEAM PROVIDES THE EXPERIENCE, EXPERTISE AND TECHNOLOGY YOU NEED

Finding a vendor with experience, expertise and technology is key

STEP 4: WHAT VENDORS AND PRODUCTS SHOULD YOU CONSIDER?

The key considerations for selecting a solution for cloud adoption and data protection are to find a vendor with experience, expertise and the technology to help you complete the step-by-step approach.

Veeam® Software's *Availability for the Always-On Enterprise*™ is an innovative solution. The Gartner, Inc. analyst firm recently positioned Veeam within the Leaders quadrant in the July 2017 Magic Quadrant for *Data Center Backup and Recovery Solutions* for the second consecutive year. Veeam improved on its *Completeness of Vision* and *Ability to Execute* in the Leaders quadrant and ranked fourth as the largest 2016 global *Backup and Recovery Software vendor for Storage Management*, behind Veritas, IBM and Dell. This positions Veeam as the vendor of choice for enterprises across the globe.

"Veeam succeeded in making us agile."

–Anders Harder, Team Manager of IT Server Operations at JYSK Nordic

LEGACY BACKUP VENDORS NOT UP TO THE TASK

"We believe that our Leadership position further proves that legacy backup vendors are losing relevance and appeal in this digital transformation era," said Peter McKay, Co-CEO and President of Veeam. "We believe our upward movement to the right [in the Gartner Magic Quadrant] is the biggest advancement in both Vision and Ability to Execute, and feel it's validation of our efforts as we drive ahead as a leader in Availability solutions for the enterprise with multi-cloud and hybrid cloud environments. You don't average 4,000 new customers each month if your product isn't reliable, rich in features and functionality, and supports the needs and demands of today's 24.7.365 Digital World. With the release of the new Veeam Availability Suite™ v10 expected early next year, Veeam will continue to innovate, execute, and drive our vision by providing customers with purpose-built solutions while also strengthening our partnerships to address a cloud-centric future."

WHAT VEEAM CUSTOMERS ARE SAYING

"For Mercedes-Benz Turk IT Infrastructure and Operations Department, the team's top priority is to ensure full time (24.7.365) Availability for the datacenter services," said Tolga Aşık, Data Center Infrastructure Specialist at Mercedes-Benz Türk A.Ş. "Veeam's contribution has not only been in backup processes but, in their end-to-end solutions with an innovative approach for the Always-On business. With numerous and inventive data recovery options, Veeam provided Mercedes-Benz Turk with the ability to reduce hours of data recovery to minutes. One of Veeam's intelligent features, file recovery, made it possible to recover a file within few minutes."

"Before we deployed Veeam, our IT infrastructure wasn't agile enough to support rapid changes demanded by the business and ensure fast time to market," said Anders Harder, Team Manager of IT Server Operations at JYSK Nordics, part of JYSK GROUP, a global retail company that sells furniture and accessories for the home. "Veeam succeeded in making us agile. We secured 24.7.365 Availability of critical IT assets and assured the business we can fully support their time-to-market requirements."

"The systems that help us provide patients with the finest care and protect their privacy are up and running at all times, thanks to Veeam," said Greg Johnson, Manager, I/S Systems Engineering Greenville Health System. "This includes Epic, the driving force of our health care system and the centerpiece of our digital transformation strategy, as well as document management, patient identification tracking and laptop encryption."

Find out more www.veeam.com

VEEAM