druva

Six steps for moving on-premises data protection to the cloud

Many organizations struggle to scale outdated tape-based backups and redundant capacity as the amount of enterprise data that needs protection skyrockets. In response, they adopt cloud-first strategies, moving from traditional solutions to cloud-native backup and recovery that can deliver significant cost reductions and performance benefits. But this requires thoughtful planning. ***This checklist outlines key strategies for CIOs to consider—and pitfalls to avoid—when transitioning data protection operations to the cloud.***

Step 1: Inventory your workloads

Review all the data you'll need to back up and where it resides, whether it's in data centers, regional or branch offices, or somewhere in the cloud. If you use SaaS applications like Office 365 or Salesforce, be sure to include those as well, since most SaaS providers recommend third-party solutions to backup business data. Lastly, don't forget to include end-user data, especially on mobile devices.

Step 2: Check your requirements

Identify your data protection requirements. Consider:

- How fast do backups need to be? What are your current SLAs for recovery point and recovery time objectives (RPO and RTO)?
- How much of your data is mission critical, and what kinds of data sovereignty and data privacy regulations do you need to comply with?
- What do you want your total cost of ownership (TCO) to look like?

Step 3: Decide how much cloud you need

Depending on your needs, you may move some or all of your data protection into the cloud. A hybrid cloud solution may offer the peace-of-mind of on-premises infrastructure, but it's likely to be the most expensive option due to hardware costs. Cloud-enabled products may be more difficult to manage since they weren't designed for the cloud. Cloud-native solutions can offer greater security and scalability and lower TCO.

Step 4: Consider the cost

If you have determined your cloud architecture and identified one or more service providers, you probably have enough information to figure out what your new cloud data protection model is going to cost. Some cloud services offer subscription-based pricing based on consumption. Your service providers should be able to provide a cost calculator to help you estimate your payments under different pricing models.

Step 5: Try cloud data protection for yourself

The only way to truly feel right about a solution is to see it in action in your own unique environment. With any approach, you want your IT group's enthusiastic buy-in, and a trial is the fastest and easiest way to get it. You can assess ease-of-use, scalability, security, as well as coverage. Cloud-native solutions have no hardware, so you can set up a trial in less than 30 minutes in most cases.

Step 6: When it's time to decide

Choosing to trust your enterprise data with a particular cloud-native data protection and management solution isn't that complicated. Does the product do the job you need it to do? Has the provider proven their character and corporate strength over time? Can you make the numbers work?

Learn why more and more enterprises are moving their data protection to the cloud in our CIO's guide to cloud-first data protection.

druva

Sales: +1 800-375-0160 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital and Nexus Partners. Visit Druva and follow us @druvainc.