Four Cloud Data Protection Appliance Considerations

2017 might well be the year that backup and recovery went from being viewed as a corporate insurance policy for data to a key business enabler and for good reasons. Natural disasters and ransomware attacks have heightened the need for fast, reliable backups and recoveries while new backup product architectures are changing the conversation around what services that cloud data protection appliances can deliver. As organizations go to select one of the current generation of cloud data protection appliances, here are four considerations they should keep in mind.

1. ***Scale-up vs scale-out architecture.*** Enterprise cloud data protection appliances use two architectures to add capacity: scale-up and scale-out. Scale-up appliances start with a fixed amount of capacity, memory, and processing but give enterprises the flexibility to add more capacity in two ways. The appliance may have extra, empty slots inside the unit where enterprises may insert additional hard disk drives (HDDs) into them. Alternatively, enterprises may add on storage capacity on external expansion units. Scale-out architectures gives enterprises the flexibility to add more capacity, memory, and processing by using preconfigured nodes with much higher capacity limit. Further, scale-out architectures simplify upgrades and ongoing maintenance. Products from Cohesity and Rubrik exemplify these new cloud data protection architectures.
2. ***Support for multiple clouds.*** The first generation of cloud data appliances primarily connected to a proprietary or reseller cloud services using them as a backup target. This has changed. All cloud data protection appliances now support connectivity to cloud

storage providers with the majority of them abandoning proprietary cloud services providers in favor of public cloud storage providers such as Amazon S3, Google Cloud, and Microsoft Azure. Having access to multiple cloud storage providers gives enterprises the option to tier backup across multiple providers. This approach helps to control costs as well as optimize data placement for applications based on each application's specific archiving, backup, data classification, data retention, and/or recovery requirements.

3. ***"White glove" recovery options.*** A number of cloud data protection appliance providers such as Carbonite and Unitrends offer "white glove" services options that provide proactive, "hands-on" services to guide enterprises through local and/or cloud-based recoveries and restores. Unitrends, for example, offers services guaranteeing 1-hour virtual machine service level agreements (SLAs), Recovery Assurance and automated disaster recovery (DR) testing.
4. ***Data mining and classification.*** While enterprises primarily create backups to perform recoveries, they now increasingly recognize these backup repositories are an invaluable resource for enterprises to use to classify and mine data. Albeit slowly, more appliances are moving down this path of indexing the data in backup repositories to help enterprises classify, understand, and derive value from the data that reside there with solutions from Veritas leading the pack in this area.

The introduction of cloud-based backup targets, technologies, and recoveries into the backup process has permanently altered how companies view data protection. Today's cloud data protection appliances reflect this new reality. Enterprises may choose appliances based on multiples factors including their support for scale-up or scale-out architectures, multiple cloud services ranging from using the cloud as a backup target to doing full recoveries in the cloud, and even

selecting providers that can walk you through disaster recoveries with their white glove services. Choose the right cloud data appliance for your environment today still demands that enterprises understand their technical requirements but now, more so than ever, they can examine how well these appliances map back to their business needs as well.