REPORT REPRINT

Data recovery matters, even for noncritical workloads

AUGUST 7 2019

By Henry Baltazar, Liam Rogers

Data is a valuable resource and the volumes of it being managed by enterprises are growing rapidly, making this data growth both a blessing and a curse. Organizations have high expectations when it comes to recovering from downtime and how much data they are willing to lose, even with less-critical apps and their data.

451 Research®

Introduction

The industry regularly waxes lyrical about the value of data, but in our Voice of the Enterprise: Storage data we see that organizations have considerable expectations when it comes to how much data can be lost in an outage and how quickly data or workloads must be recovered. While there is a clear and logical hierarchy in importance between mission-critical, business-critical and noncritical applications and data, many organizations are unwilling to tolerate long periods of downtime for even noncritical data.

451 TAKE

Enterprises and smaller organizations are unwavering in their demands when it comes to recovering workloads and data critical to their business and overall mission. The price of downtime and data loss can be massive and costly outages regularly make headlines. There is higher tolerance for downtime on noncritical apps and data, but for almost half of customers, the RTO (Recovery Time Objective) expectations of less than a day demonstrate that even less-critical apps and data are important and require rapid recovery. Additionally, enterprises will need to move toward data management practices that encompass not just the backup of applications and data but also the ability to restore them quickly after outages as well as make the data available to the business so that insight can be derived from analytic and machine learning endeavors, regardless of whether they exist on-premises or in the cloud.

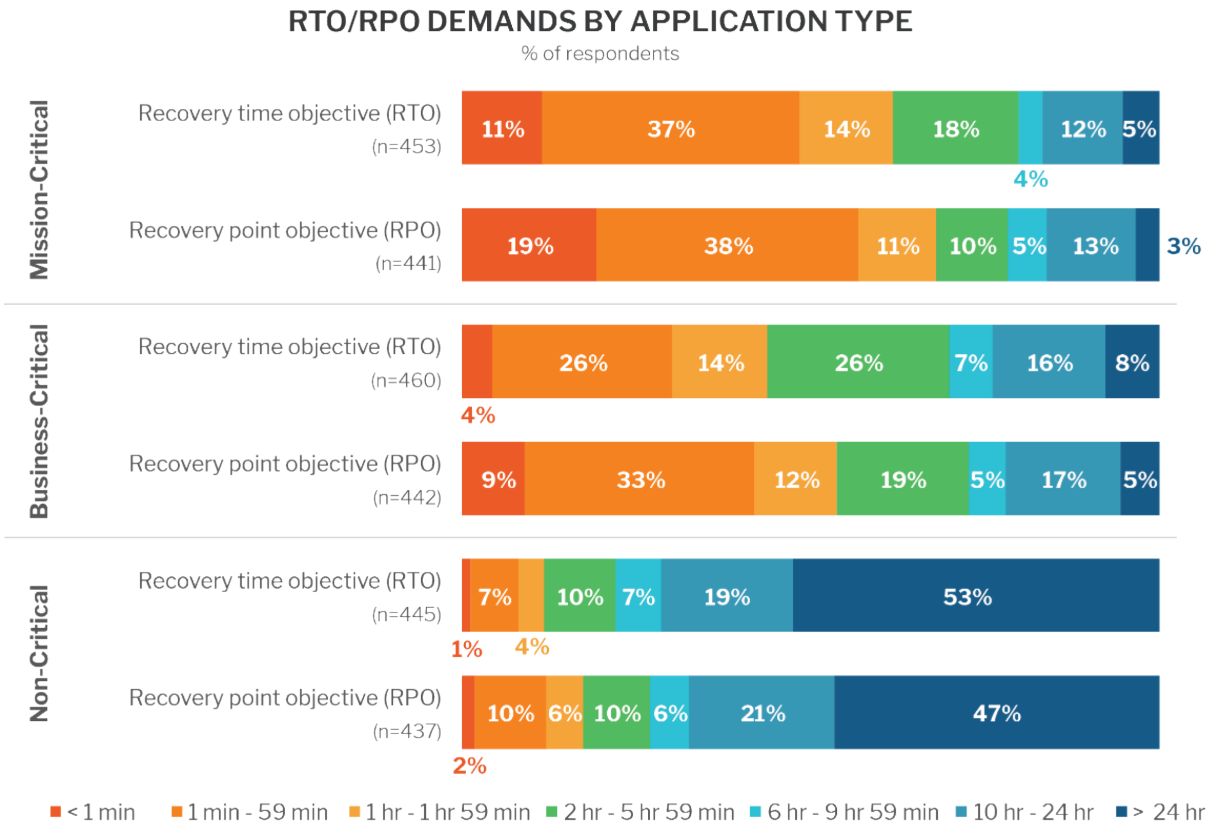
RTO and RPO expectations are high

RTO and RPO (Recovery Point Objective) are both metrics used in disaster recovery planning. RTO is the metric specifying the amount of time that is permittable for a recovery operation to complete; effectively, the amount of downtime that is acceptable for a given application or workload. RPO is the metric that measures the acceptable amount of data that can be lost as a result of an outage. Logically, RTOs and RPOs shift based on the criticality of the workload being recovered; the more critical the workload, the lower the tolerance for downtime.

In our Voice of the Enterprise: Storage, Workloads and Key Projects 2019 report, we see that almost half (48%) of organizations have current RTOs for mission-critical application of less than an hour and this number is 30% for business-critical apps. Similarly, 57% of organizations have RPO demands in the sub-hour timeframe for mission-critical apps and data. For noncritical apps and data, the tolerance for recovery in the 24-hour-plus range is considerably higher than more critical workloads, but a substantial number of customers expect RTOs and RPOs of less than a day (47% and 53%, respectively) – and this shows that daily backups alone are not good enough even for noncritical workloads, and organizations will need to implement snapshot and replication technologies to meet these more stringent recovery requirements.

Figure 1: RTO/RPO demands by application type

Source: 451 Research, Voice of the Enterprise: Storage, Workloads and Key Projects 2019



Secondary storage doesn't end at backup and DR

The volume of unstructured data being generated (in our study on Storage Budgets and Outlook, data/capacity growth was the top storage pain point at 45%) makes the task of backing up and restoring data all the more complicated. This is also exacerbated by hybrid and multi-cloud because workloads and data cover a larger expanse that must be managed. Then add in the desire for organizations to actually make use of all this data for insight-producing endeavors such as analytics and machine learning. To meet these needs, secondary storage vendors need to provide not just backup and DR for short- and long-term data retention, but broader data management to secure, protect and make available the large data volumes enterprises are retaining so that organizations can have visibility into the data that they have and so that it can be used to create actionable insights to improve the business.

This includes data protection products in the portfolios of the main storage incumbents: Dell EMC (Data Protection Suite), Hitachi Vantara (Data Protection Suite), IBM (Spectrum Protect Suite), Micro Focus (Data Protector) and NetApp (NetApp Data Availability Services). Smaller companies that round out this space include the likes of Acronis, Actifio, Carbonite, Code42, Cohesity, Commvault, Rubrik, Veeam, Veritas and Zerto.

As usage of cloud-based applications increases, enterprises must also consider the protection and management of data tied to SaaS applications. Although it varies from vendor to vendor, SaaS providers tend to offer basic data retention and we've seen two years running that the majority of customers are not taking steps to protect their SaaS data, with 52% of customers relying on their cloud vendor for backup and recovery and 22% not backing up SaaS apps at all. Aside from some vendors already mentioned, companies taking on the backup of SaaS data include Asigra, Barracuda Networks, CloudAlly, Cloudfinger, CloudHQ, Clumio, Druva, Metalogix Software, Spanning Cloud Apps (acquired by Kaseya in 2018), SkyKick and StorageCraft. Currently our data shows that only 8% of organizations are using a cloud-cloud backup provider, showing that this is a nascent space with lots of growth potential, and larger vendors like Veeam have begun to make inroads here.