Enterprise Data Protection Strategy to Improve Recoverability

When my smartphone died, replacing it was easy. I simply went to the nearest phone provider for a replacement. But, that's only half of the story. As luck would have it, it died just when I was leaving for an important business trip. What was I to do about my stored data? I didn't have time to recover all of my data, so I had to prioritize the data that I needed. What data is most important to me? Contacts? Email? Banking App? Company Apps? Airline App? Ridesharing App? Social Media App? Food Delivery App? 5000 photos?

The answer: some of the above. I restored the critical data I needed to make my smartphone useful, and then I took my time to restore the rest of it.

Consider how this scenario applies to you and the organization you work in, albeit on a much larger scale. Some of your data may be "mission-critical," when, if not available, could be costly and compromise your business, from a revenue, customer, and brand perspective. A recent study by Enterprise Strategy Group (ESG), who researched the implications of application downtime[1], found that loss of revenue had the most impact to an organization where application downtime or lost data has occurred.

Apart from scale and cost, there are threats. Traditional IT threats, such as failed upgrade and human error, have increasing potential effects with exponential data growth and the rising amount of data managed per administrator. And there are a host of new, insidious threats to contend with, with cybercrime on the rise

and climate change making weather patterns extreme and unpredictable.

Don't forget the backdrop to all of this. With digital transformation, customers have high expectations of the organizations that they do business with. Not only do customers expect applications to be 24/7 "always on," but they expect fast responses with a highly personalized experience.

So what does this mean for an enterprise data protection strategy?

Restore over Backup

Organizations must transform their thinking from backup to restore. It's logical to think about backup. More data is backed up than is restored. But, given the increasing business value of data and the cost of downtime, restore is more critical than backup.

One Size Does Not Fit All

Organizations must identify their mission-critical data and the associated costs to their business of not having that data available, and evaluate technologies that can meet the restore SLAs.

The Critical Role of Backup Software in Data Protection

Backup solutions have long been the mainstay of Enterprise Data Protection. Over time, they have evolved to become the control plane – administration and cataloging – and also integration with third-party solutions.

Backup Technologies

There is a wide range of mature technologies to help you meet your applications' restore SLAs. An enterprise data protection strategy will define the SLA that the business requires for each application and match it to the right backup technology.

Before we outline the technologies that you can deploy, it's worth taking the time to look at common terminology and the backup capabilities of a few of the different technologies available.

- **Recovery Point Objective (RPO): This is defined as *"your company's loss tolerance: the amount of data that can be lost before significant harm to the business occurs"*** [2]
- **Recovery Time Objective (RTO):** This can be defined as "*how much time an application can be down without causing significant damage to the business*"[2]

Replication Technologies

Storage vendors have been providing these technologies for some time. This allows storage to take copies while in production and send those copies to alternative storage, often in a different location. Integration is also provided for the applications, allowing the application to use the alternative copy if failure occurs.

Advantages	Disadvantages
Highest level of RPO and RTO	Incurs additional cost and complexity
	May not be suitable for all applications
	Doesn't protect against all failures (e.g data corruption)

Hardware Snapshots

They have been provided by hardware array vendors as a very quick way of providing a recoverable copy

of an application. Snapshots, also known as or clones, can be created in seconds with little performance impact on the application, and they are typically attached to the storage array from which they're created.

Multiple snapshots can be generated throughout the day, which greatly improves the recovery point objective. For example, I can make copies of my mission-critical database every hour so I can recover back to the hour. I can also accelerate my recovery time objective by replacing the live data with my snapshot.

Advantages	Disadvantages
Excellent RPO & RTO	Some compatibility / interoperability challenges
	Can incur additional license & storage cost
	Still need to take a copy of the snapshot

Disk-based Backup

Disk-based backup has been in use for many years, but its uptake accelerated with the advent of more cost-effective SATA disk in the early 2000's. This allowed organizations to introduce "disk" staging, where backups would go to disk first and then be moved to tape for long-term storage.

Advantages	Disadvantages
Improved RPO & RTO over tape	Scalability
Simple to implement	Still need second copy for disaster recovery
	As disk capacity grows, management is becomes complex

Disk-based Backup Appliances

After the significant use of SATA disk for backup, the backup environment was disrupted in the mid to late 2000's by Purpose Built Backup Appliances (PBBAs). These appliances delivered deduplication which enabled organizations to store less backup data (only unique data is stored) and also protect remote offices (only unique data is sent). A later development saw backup software included with appliance providing a full turnkey solution.

Advantages	Disadvantages
Easy to deploy	Recovery time increases as more data is backed up
Simple to design	Dedicated to backup & recovery only
	Creation of data "silos" that increase complexity

Tape

Tape technology has long been the mainstay of Enterprise data protection. Prior to backup appliances, data would sent via network from primary storage and written to tape. Often tapes were duplicated and one or more copies were shipped off-site to a second location. When backup appliances became popular, tape was typically only used as the disaster recovery copy.

Advantages	Disadvantages
Most cost efficient per TB stored	Manually Intensive
	Durability challenges (tape / device wear)
	Poor RTO

Public Cloud

One of the most common use cases of public cloud is to be a long term repository for backup data. Backup software vendors have built various layers of integration with public cloud vendors so backups can be sent to the cloud for storage. Public cloud is replacing tape as a means of providing a disaster recovery copy.

Advantages	Disadvantages
Simplifies providing offsite copies	Cost increases depending on retention & access
Backup data is reusable by cloud apps	Potential local data residency restrictions
High levels of durability	

There are several technologies available to help organizations meet their data protection requirements. However, according to 451 Research, recovery continues to be a top concern for organizations. Most importantly, expectations for data recovery are extremely high, even for non-critical workloads: data warehouses, analytics, and AI applications, for example. One reason for this is that organizations are starting to see real examples of the competitive advantage that their data can provide them.

With organizations becoming more and more reliant on their data, not only to run their businesses but to gain competitive advantage through analytics and machine learning, the recoverability of data has never been more important. Whilst there are many different technologies that can help recover data, it's important that organizations understand the role each technology can play in an enterprise data protection strategy.

Are you looking to overhaul your Enterprise Data Protection strategy to improve your overall recoverability? Do you need to understand the implications to your organization of not being able to provide the level of recoverability that your customers need? Take a look at the latest research from 451 and then read Data Protection in the Age of Always-on Workloads.

References

1. "Crossing the Data Management Chasm: From DR to Data Intelligence," Christophe Bertrand, ESG
2. "RPO and RTO: Understanding the Differences," Enterprise Storage Forum