Economic Insight Paper

Using Self-Protecting Storage to Lower Backup TCO

A TCO comparison of NetApp’s integrated data protection solution vs. a traditional backup to an external PBBA

By John Webster, Sr. Analyst

October 2017

Evaluator Group

Enabling you to make the best technology decisions

Modern Approaches to Assuring Critical Data Integrity and Availability

Enterprise IT is undergoing a transformational process that is impacting every level of the organization. Cloud computing now dominates many new project agendas as business user groups gravitate to cloud-based applications. And as enterprise IT responds with new service delivery capabilities, the traditional application environment can't be ignored or neglected either. As a result, IT is challenged to drive operational efficiency as it strives to achieve a balance between the new cloud and traditional IT environments without incurring a budget-breaking increase in infrastructure and headcount.

One place IT can look to for gains in operational efficiency is the data protection function which is critical to both traditional and cloud environments. In fact, cloud computing places additional demands on an enterprises' existing data protection capabilities. When these additional demands are examined, there emerges a clear need to transform current practices. Unfortunately, this can result in a struggle for budget dollars that pits new business aspirations against IT processes that don't produce revenue. Funding for advancing data protection with replacement technologies and solutions may be hard to find.

A cost-efficient way to inject new data protection practices that are commensurate with business advancement projects is to use integrated data protection capabilities built into modern data center storage systems. Doing so makes the effort an incremental process which is tied to other, broader business advancement objectives. Here we outline NetApp's SnapMirror approach to data protection and compare it on a TCO basis to what has become the traditional practice of using an external data protection system such as a purpose-built backup appliance (PBBA) with additional backup software.. We note that similar results can be seen as compared to the even more traditional approach of tape-based backup and restore. However, analysis of tape systems is beyond the scope of this report.

The Value of Self-Protecting Storage

Self-protecting storage where storage systems have the capability to make protected copies of information on target data protection storage is a major advancement in enterprise data protection that promises to enhance data availability and integrity while reducing cost in the following ways:

> *Reduce or eliminate* the need to acquire additional secondary storage resources that use faster devices to complete backups within acceptable backup windows as data volumes grow. These resources include backup servers, storage capacity, software licenses and administrative staff time.
>
> *Avoid shutting down* or pausing applications during the protection process—a practice that is increasingly unacceptable in "always on" business environments.
>
> *Automate the tiering* of data protection copies so that the most recent are immediately available when needed. This allows storage administrators to meet stringent recovery time objectives (RTO). Tiering of non-active data to cloud is also supported.

Implementing self-protecting storage also results in significant improvements in a storage administrator's recovery point objectives (RPO) and recovery time objectives, the benefits of which are discussed in more detail later-on in this report.

Reducing Data Protection System TCO

Traditional data protection systems are typically a conglomeration of point products—often from different vendors—that are bought, managed, supported, and tracked separately because each has its own technology lifecycle to be concerned with. Depending on the capacity and scope of the data protection environment, the hard cost of point products can include a purpose-built backup appliance (PBBA), data protection software and associated servers, dedupe appliances and cloud gateways when a link to off-site cloud storage is required. Additional costs that are harder to quantify, but are nevertheless very real include:

- Managing a complex environment
- Increased risk of downtime due to multiple points of failure
- Technology update and refresh cycles applied to each of the components that escalate over time.

Using self-protecting storage, costs devoted to point product architectures are greatly reduced if not eliminated as is the case with a PBBA or Tape. Costs for technology and capacity upgrades, once devoted solely to data protection, now become part of the ongoing support costs for primary and secondary data storage. The result can be a dramatic reduction in TCO for data protection systems. Here we analyze the economic impact of this shift using an implementation of NetApp's SnapMirror as an example.

Self-Protecting Storage using ONTAP and SnapMirror

NetApp FAS and All-Flash FAS (AFF) systems with ONTAP offer the integrated replication engine SnapMirror that can be used as a self-protecting storage feature. It provides automated data protection capabilities and features block-level incremental backups.

SnapMirror supports the use of a second ONTAP system as a backup target, eliminating the need for a separate PBBA, backup server and related software. When a second ONTAP system is used as a target in mirroring mode, it allows administrators to take multiple data copies on the primary (protected) NetApp array and aggregate them to a secondary (target) NetApp array, only sending incremental block-level changes that are already compressed and deduped over the network to help improve CPU performance and hold down TCO. In vaulting (or backup) mode, SnapMirror replicates incremental changes from the source to the destination at specified, regular intervals. Backup performance is also improved when SnapMirror is used in conjunction with a secondary FAS array as a backup target, thereby eliminating the backup server/software, tape systems and an associated backup appliance as is traditionally used.

SnapMirror supports the storage of multiple asymmetric copies on the secondary NetApp system allowing IT administrators to keep weeks of backups that are immediately available for online restoration as needs arise. SnapMirror also allows administrators to choose which primary system to back up/mirror and how frequently.

After the data is replicated either internally or to an external storage system in native format, it can be accessed immediately to restore the data to the source in the event of a disaster, data corruption, or user error. Copies of data can also be cascaded to tertiary FAS or AFF systems, tape or cloud or cloned for dev/test scenarios.

TCO Comparisons of Self-Protecting Storage vs. Traditional

To demonstrate the economic value of self-protecting storage, we built two TCO models that compare the costs of using NetApp SnapMirror to create and store data protection copies to those using traditional backup and recovery software in one case, and those using both backup software plus a PBBA in another.

The impact to TCO of the NetApp SnapMirror solution is shown in the following yearly TCO analysis where:

- A NetApp All Flash FAS (AFF) system is used as the source (primary) of data to protect
- A NetApp FAS system (blue) or a purpose-built backup appliance (PBBA-red) is used as the target data protection storage
- Backup software is used to generate the backup streams to either the target FAS system (black) or the PBBA target (red)
- The data protection process typically creates:
    - Full backups four times per month
    - Incremental backups once per day
    - Snapshots 5 times per day
- The cost for data protection includes hardware, software and staff support
- In this TCO analysis, the source capacity was 100 TB with a 10%/year growth rate

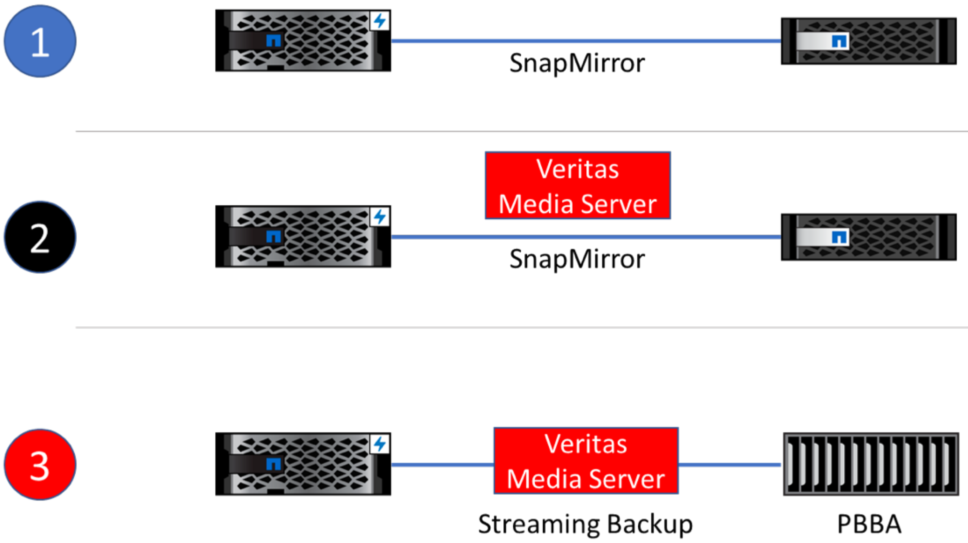

Figure 1. Source and target configuations used in the TCO analysis in Figure 2 below where configuration 1 is a NetApp All Flash FAS (AFF) array to a secondary NetApp FAS array using SnapMirror (blue); 2 is the backup of an AFF array to the same secondary using Veritas NetBackup (black); and 3 is the backup of the AFF array to a leading PBBA using NetBackup (red).

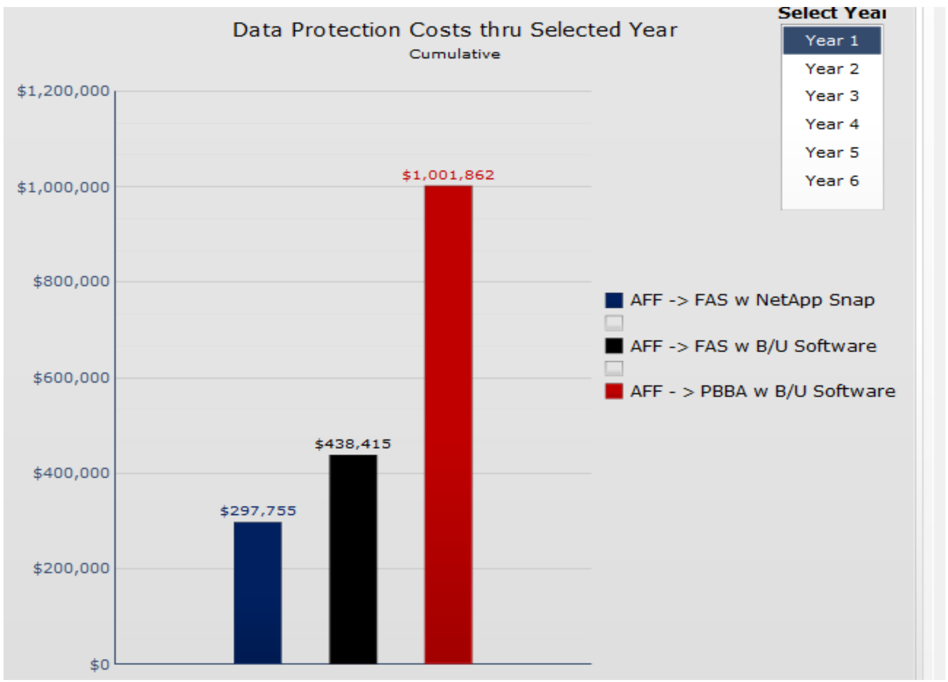

Figure 2. First-year total data protection costs comparing the configurations presented in Figure 1 above. Configuation 1 is represented by the blue bar; configuration 2 by the black bar; and configuration 3 by the red bar.

We note that a 33% TCO savings can be realized in the first year of operation by using SnapMirror instead of traditional backup software to create a backup data stream to the secondary FAS system. When we replace the PBBA as the target and eliminate the use of backup software, a TCO savings of 70% can be achieved when using a secondary FAS systems as the target .

In Figure 3 below, we make the same system comparison with the same assumptions as above but show the cumulative impact to TCO over a six-year period. However, in this case, upgrades and hardware refresh cycles are taken into consideration.

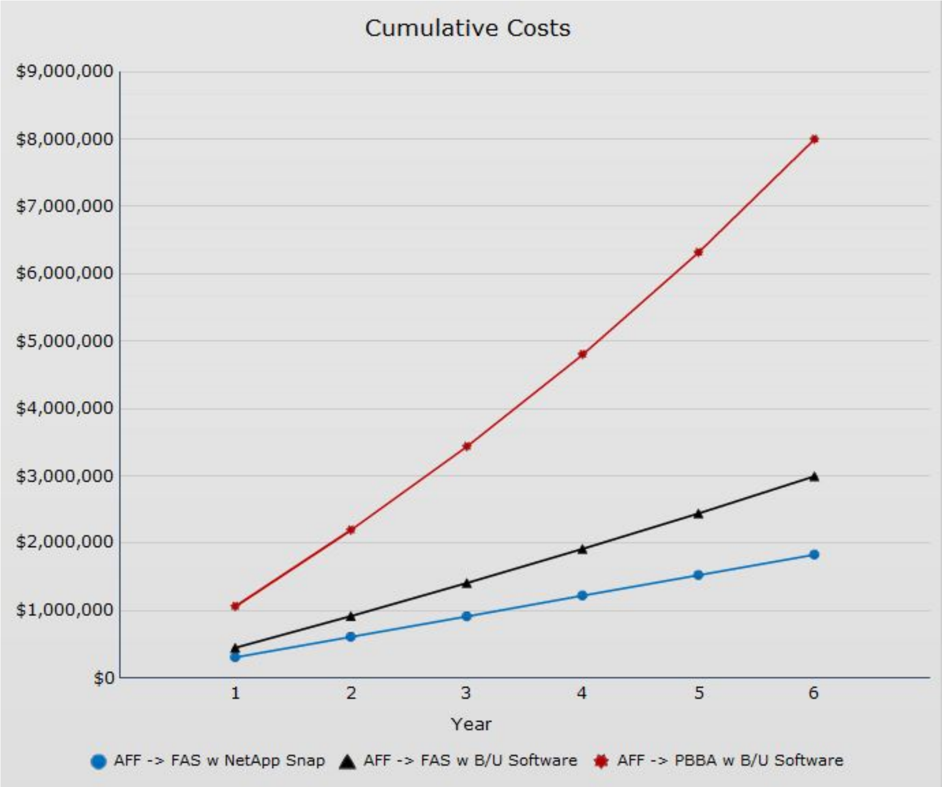

Figure 3. Six-year cumulative TCO using the same system comparisons where backup of a NetApp All Flash FAS (AFF) array to a secondary NetApp FAS array using SnapMirror is shown in blue; backup of the AFF array to the same secondary FAS array using Veritas NetBackup is shown in black; and backup of the AFF array to a leading PBBA using NetBackup is shown in red.

In Figure 3, we note again that a 40% TCO savings can be realized over a six-year period of operation by using SnapMirror instead of traditional backup software to create a backup data stream to the secondary FAS system. When we eliminate the use of backup software and replace a PBBA as the target with the secondary FAS system, a TCO savings of 75% can be achieved. A breakdown of costs used to generate our modeled results is shown in Figure 3 below.

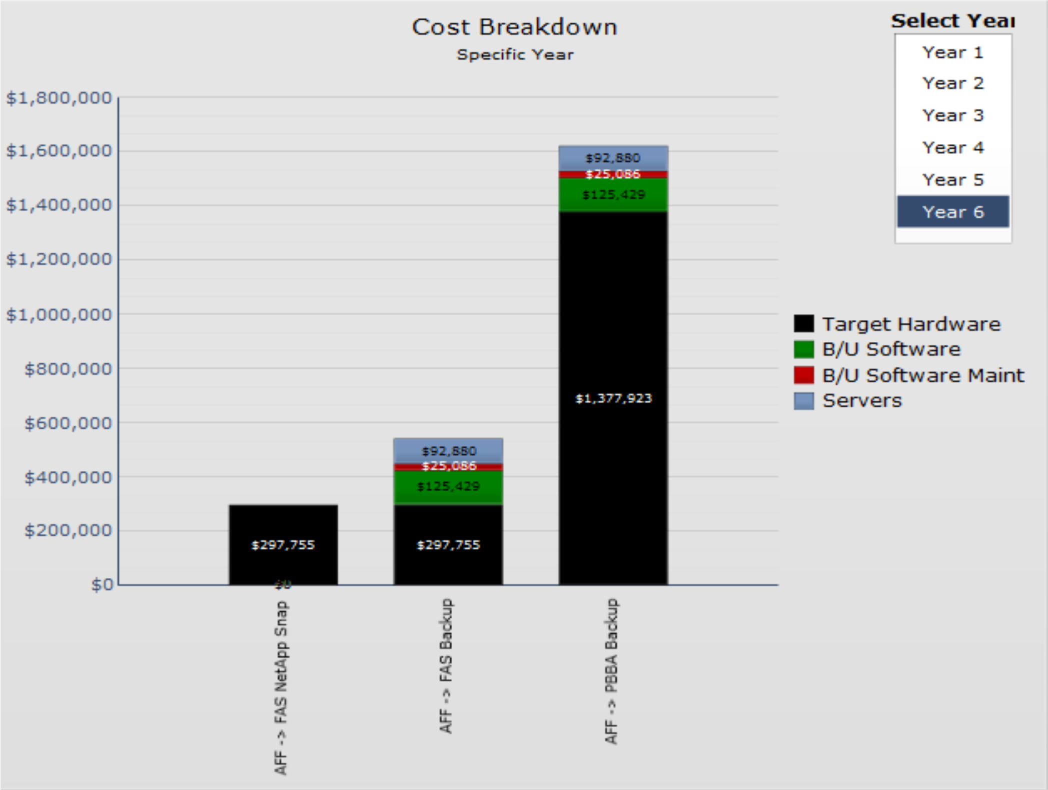

Figure 4. Breakdown of costs used to compile the comparison data shown on Figure 3.

Recovery Point Objective (RPO) Impact

While an economic assessment of the impact to recovery point objectives resulting from self-protecting storage is difficult to quantify, it is at least worth an analysis by IT administrators who are familiar with their often unique environments. Establishing an acceptable time interval for data loss exposure sets the RPO. Assume that a recovery is performed 14 hours after a backup was created. The enterprise is exposed to the loss of data changes that occurred during that time interval.. Decreasing the time interval lessens the exposure. However, a premium is normally paid to get data protection systems capable of reducing exposure. The result is an increase in TCO to achieve more immediate RPOs..

Using SnapMirror for the protection of the primary NetApp system data can result in a significant improvement in an IT administrator’s RPOs. Storage administrators can simply make the target FAS system writable so administrators can use the target volume the last time data was copied to effect a recovery.

Reducing the time intervals between recovery points reduces data loss exposure that could negatively impact revenue and customer satisfaction depending on the circumstances. Each enterprise is impacted differently by data loss. However, every enterprise storage administrator is critically aware of its impact.

The following Figure 5, which is based on the same parameters used in the previous analyses shows that the same NetApp solution yields a significant improvement in RPO with no additional cost.

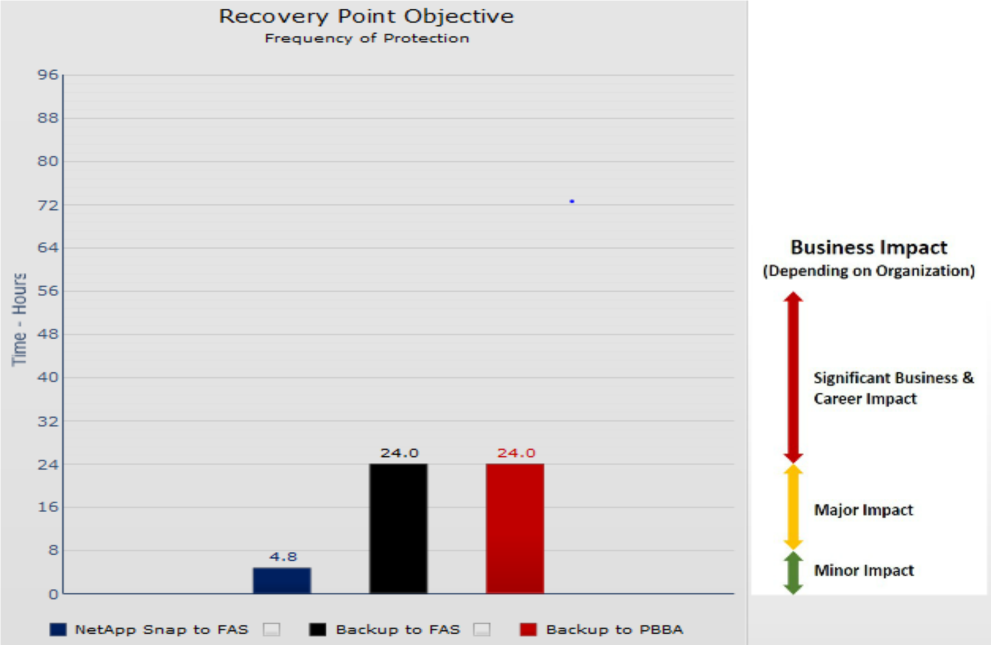

Figure 5. Comparison of Recovery Point Objective (RPO) time intervals (in hours) with an assessment of relative risk exposure (minor, major, significant) of the solution scenarios modeled in the previous TCO analyses and using the same parameters.

Conclusion

Using self-protecting storage, it is now possible to transition data protection practices and systems away from using external PBBA and specialized software to a more cost-effective solution that leverages existing storage array infrastructure. This results in the following major benefits:

- The TCO for data protection systems is reduced
- Backup and recovery performance is accelerated
- Data protection storage capacity growth is more sustainable
- Existing data protection levels are less threatened by high rates of capacity growth
- Exposure to data loss is reduced without a significant additional investment in storage resources

In summary, we have demonstrated that NetApp's SnapMirror software can substantially reduce data protection costs for its All Flash FAS systems used as primary storage arrays as well as reduce risk exposure to inadvertent or disaster-related data loss.

About Evaluator Group

Evaluator Group Inc. is dedicated to helping ***IT professionals*** *and vendors create and implement strategies that make the most of the value of their storage and digital information. Evaluator Group services deliver* ***in-depth, unbiased analysis*** *on storage architectures, infrastructures and management for IT professionals. Since 1997 Evaluator Group has provided services for thousands of end users and vendor professionals through product and market evaluations, competitive analysis and* ***education****.* ***www.evaluatorgroup.com*** *Follow us on Twitter @evaluator_group*