

## Product Brief

# NetApp Modernizes Backup

**Date:** June 2011 **Author:** Lauren Whitehouse, Senior Analyst

**Abstract:** [NetApp](#) has stepped up efforts to deliver a more comprehensive data protection solution for NetApp and non-NetApp storage environments. The company extended its capabilities via partnerships with [Syncsort](#) and [CommVault](#), augmenting its base data protection features to meet current and prospective customer requirements.

## Overview

The basic goal of data protection is to mitigate risk by preventing or minimizing business disruption and financial loss. That means that systems, applications, and data should maintain a consistent state of operations and, if interrupted, be returned to their most recent and consistent state before the downtime event within a pre-established timeframe. Creating duplicate (backup) copies of data is a means to that end.

Unfortunately, there are forces working against the people, processes, and technology in place to accomplish this. A big one is data growth: growth in the volume of data creates challenges with time (to make copies and recovery them), cost (for the infrastructure to capture and maintain backup copies), and risk (more data and dependence on data could create vulnerability). Since time is fixed (only 24 hours in a day), organizations have to either spend more or lower their standards and potentially increase risk.

Disk-based backup has been the antidote to the too-much-data-to-copy-in-a-fixed-time-window problem. Over the last few years, the focus has been on the optimization (acceleration) of the “writing” portion of the backup process. There’s been less focus on the “capture” aspect of making duplicates—especially by traditional backup applications.

This has not been the case with NetApp. NetApp’s data protection portfolio is not conventional. The company’s approach is based on snapshot copies and mirroring—leveraging efficient incremental block-level data capture and transfer. However, there are a few drawbacks that some organizations have objected to with NetApp’s method:

- **Lack of catalog and search capabilities** – while snapshots can be mounted and browsed for desired data, data that is indexed and searchable is preferred.
- **Inability to create tape-based copies** – while NetApp can duplicate copies locally or remotely via replication, organizations requiring long-term retention often prefer physical tape media due to its lower cost and portability.
- **Limited to homogenous storage environments** – NetApp’s data protection strategy is limited to NetApp’s own storage environments.

It’s these requirements that NetApp is addressing with its Integrated Data Protection (IDP) strategy, a two-pronged approach that leverages NetApp-only solutions and those belonging to NetApp’s leading backup providers. So far, NetApp announced partnerships with Syncsort and CommVault for the latter, delivering simple, high-speed, and efficient backup and recovery operations.

## Analysis

### NetApp’s Portfolio

NetApp’s solution for disk-based data protection is comprised of several components and is based on snapshot copies, remote mirroring, and centralized administration and policies. Storage capacity and bandwidth are optimized with block-level updates and network compression after the initial copy is made. The portfolio includes:

**NetApp Snapshots** – point-in-time copies of data volumes that consume only a fraction of the space normally required with backup copies.

**SnapRestore** – enables rapid recovery of data from a NetApp snapshot made at an earlier point in time.

**SnapVault** – creates point-in-time, read-only versions of a data set and stores them in native format on a SnapVault secondary system.<sup>1</sup>

**Open Systems SnapVault (OSSV)** – performs point-in-time snapshots of an open system’s filesystem and replicates it to a SnapVault system

**SnapMirror** – replicates (synchronously, asynchronously, or semi-synchronously) a local snapshot copy to one or more secondary storage systems.

**MetroCluster** – combines synchronous mirroring within or between sites and array-based clustering to enable automatic failover of any single component or a site.

**SnapLock** – “locks down” files on NetApp arrays to prevent deletion or modification of data for a specified retention period to meet compliance mandates for retention.

**SnapManager** – available for applications such as Oracle, SAP, VMware, Citrix Xen, and Microsoft SQL, Exchange and SharePoint, it integrates NetApp data protection products with the application/hypervisor APIs.

**Protection Manager** – provides a management and monitoring interface, and the ability to automate SnapVault, OSSV, and SnapMirror operations based on user-defined policies.

**Deduplication** – a native component of NetApp FAS systems, it works in conjunction with SnapVault and SnapMirror to optimize bandwidth and storage capacity by identifying and eliminating redundant data (i.e., transfers and stores only unique data).

**FlexClone** - NetApp FlexClone technology creates true clones (instantly replicated data volumes and data sets) without requiring additional storage space.

## NetApp Syncsort Integrated Backup (NSB)

NSB delivers backup and recovery for heterogeneous storage environments. The solution combines NetApp FAS disk systems, NetApp Protection Pack software,<sup>2</sup> and Syncsort management and data protection software. Syncsort creates a point-in-time backup copy by invoking SnapVault, storing recovery points on NetApp FAS storage. Syncsort provides the management and monitoring console, central policy manager, and catalog for storing metadata. Site-to-site mirroring via NetApp SnapMirror or the creation of physical tapes by BEX provide offsite copies for disaster recovery purposes.

Data can be recovered in several ways: via physical tape, catalog-searchable snapshots, or mounted snapshot images. Syncsort also enables a bootable P2V or V2V style of recovery based on a point-in-time backup image. Data recovery can be at the file, application (Exchange, SQL, SharePoint, Oracle), server, or site level.

NSB closes several of the gaps in the NetApp-only strategy by providing a solution for heterogeneous storage environments, cataloguing metadata and enabling search and restore across disk and tape, and facilitating tape media management. And it does this while introducing efficiency in backup/recovery time, bandwidth, media, and budget.

## NetApp SnapProtect

NetApp SnapProtect leverages CommVault Simpana technology to deliver a management interface to invoke, catalog, and manage snapshot copies for backup and recovery, supporting disk and tape copies. It accomplishes what NSB does, but for homogenous NetApp storage environments.

SnapProtect manages backup, NetApp snapshot, and replication across physical and virtual infrastructure and enterprise applications. For virtual environment and application-specific backup and recovery, application- and hypervisor-aware software agents are used to enable recovery in a few ways: based on the source construct (file-level recoveries from a virtual machine image and item-level recovery for an application), a full virtual machine, or VMDK. The beauty of the SnapProtect solution is that processes are managed from a central location in a single workflow: from disk to disk to

<sup>1</sup> ONTAP 7.3.2 SnapVault supports this on local and secondary systems.

<sup>2</sup> SnapVault, SnapMirror, and FlexClone are included in Protection Pack and Advanced Pack.

tape (with integrated tape media management) or disk to disk to disk (through replication management). SnapProtect catalogues copies to accelerate search and e-discovery requests. Storage efficiency features in NetApp Data ONTAP, including deduplication and compression, are available to control costs.

The partnership with CommVault to deliver SnapProtect accomplishes what the Syncsort-NetApp relationship does: it closes gaps in the NetApp-only strategy. Providing index/search capabilities and a catalogue that tracks copies across all storage tiers and locations accelerates recovery and provides customers that have a more traditional view of backup and recovery with an easier transition to a snapshot-enabled data protection approach. Since SnapProtect supports tape media, IT organizations can still rely on tape without sacrificing performance in backup processes.

## Too Confusing?

So, why did NetApp partner with two different companies? Isn't that just introducing confusion? It could, but it likely won't. On the surface, the partnerships and resulting solutions look similar, but there are a few distinctions:

- NSB is an integrated solution; however, it is packaged separately. Customers purchase components from Syncsort and NetApp via mutual channel partners. SnapProtect is a NetApp offering based on technology OEMed from CommVault and is available through NetApp and its channel partners as a NetApp product.
- NSB is geared toward smaller to mid-size environments, while SnapProtect is positioned for enterprise environments.
- NSB delivers data protection for heterogeneous storage environments, while SnapProtect is limited to protecting NetApp storage systems.
- NSB pricing is a la carte: organizations procure NetApp FAS disk systems and NetApp data protection software via a single distributor SKU. For the Syncsort component, licensing is capacity-based through Syncsort. SnapProtect is licensed on a per-controller basis with "all you can eat" functionality.

## The Bigger Truth

NetApp's efforts to strengthen its data protection portfolio are very telling about customer requirements. Data growth and the complexity in backing up live virtual machines have placed pressure on IT organizations to re-think traditional backup approaches. However, not everyone is ready to throw out the baby with the bathwater. Storage and backup administrators are "tape-huggers" and they're "white-knuckled" when it comes to managing data protection via a central policy engine and catalogue. They'll embrace change, but there's some things they just won't (or can't) let go of.

NetApp recognized this hurdle to greater adoption of its snapshot- and replication-based data protection strategy. The company had longstanding partnerships with both Syncsort and CommVault it could leverage to advance its capabilities. From this, its IDP strategy was born.

NetApp is not in the clear yet. The company has some work to do to socialize its strategy with IT professionals and channel partners, and make sure it clearly differentiates components of its IDP portfolio. If NetApp is successful in educating clients and prospects regarding the benefits of a "modern" backup approach, one would expect the company to be successful in leapfrogging several of the more traditional backup vendors whose portfolios are lagging of late—especially if NetApp's IDP strategy is combined with its a focus on virtualized environments where change goes hand-in-hand with virtualization initiatives.