

## WHITE PAPER

---

# NetBackup 6.5: Enabling Next-Generation Disk-Based Data Protection

Sponsored by: Symantec Corporation

---

Laura DuBois  
November 2007

## EXECUTIVE SUMMARY

Influenced by factors such as disaster recovery, regulatory compliance, legal pressures, and IT risk management, many IT organizations need to enhance their current data protection to improve recovery and reliability and meet compressing backup windows. The challenge most organizations face is how to upgrade their current processes in an economically viable manner without disrupting users, applications, or infrastructure. Today, enterprise datacenters are augmenting existing data protection configurations to satisfy both technical and business challenges in managing, protecting, retaining, and recovering corporate data.

Symantec's Veritas NetBackup 6.5, the latest release of the company's established market-leading enterprise backup and recovery solution, provides disk-based data protection for remote office and enterprise datacenter environments. Enabling next-generation data protection, NetBackup 6.5 provides a common platform from which firms can choose and manage a comprehensive set of cost-effective options for disk-based data protection. NetBackup 6.5 incorporates next-generation data protection features to enable higher levels of recovery, reliability, and performance while providing an economically viable and open architecture for different back-end disk configurations, all of which are managed under a common administration model to provide operational savings.

## TECHNICAL CHALLENGES

Today's backup and storage administrators, architects, and engineers face technical challenges in protecting data in increasingly distributed and dynamic corporate IT environments. These professionals need to manage not only the data protection infrastructure but also the corporate data contained within it according to budgetary and human capital constraints. While meeting these objectives, technical backup and storage professionals must satisfy the following data protection requirements:

- ☒ **Meet shrinking backup windows while facing data growth.** The amount of data requiring backup is exceeding available backup windows and is exacerbated by data growth of 52% annually. With no practices for pruning and cleanup of primary data or backup data, most firms add more backup hardware to address the problem. However, as backup windows disappear, this approach is not sufficient because there is not enough space or money to continue throwing hardware at the problem. This challenge can be mitigated by eliminating the continual backup of duplicate data, which reduces the amount of data requiring backup and thus shrinks the backup window.

- ☒ **Manage disparate, distributed data protection products.** Storage and backup administrators need to manage disparate types and numbers of data protection, replication, and backup architectures in both datacenter and satellite locations. Commonly, a large firm will have an average of three disparate backup applications, many different replication approaches, and a varied use of disk and tape media as a target for backup. These architectures are distributed across systems and vendors — often siloed by geography, business unit, datacenter, or operating environment. The disparate nature of these systems prohibits the unified management of different application-driven protection and recovery service-level agreements (SLAs). The diverse set of data protection products results in multiple management consoles and agents and can challenge consistent policies and processes. The use of a data protection platform where different technologies and functions can be applied to meet different application requirements reduces operational risk, administrative overhead, and infrastructure complexity and cost.
- ☒ **Manage and improve backup and restore reliability.** Failed backups, the result of bad media errors, closed backup windows, network errors, misconfigured systems, hardware failures, and limited tapes commonly compromise successful recovery. When identified, unsuccessful backups require troubleshooting to locate the root cause and reinitiate the backup. Restore problems can include failure to restore data on a first attempt, lengthy periods to retrieve media or data from offsite locations, and inability to meet recovery objectives with current backup approaches. Increasingly, disk-based data protection approaches can aid in improving the reliability of backups through processes such as verification, volume spanning, storage pooling, and sophisticated load balancing and failover capabilities.
- ☒ **Support virtualized server environments.** Datacenters are deploying server virtualization at unprecedented rates to aid in consolidation, utilization, and mobility in support of dynamic IT. The ease of creating new virtualized applications and systems creates pressures on storage and backup teams to keep up with data protection services while meeting compressing SLAs. Data protection environments need to detect new virtual machines and protect them in a manner that does not compromise performance, availability, and recovery expectations.
- ☒ **Protect remote and branch offices.** Large U.S. firms (those with more than 5,000 employees) have an average of 258 branch and remote offices. Often, distributed file, print, and application data is stored locally to these remote locations, while the challenges of protecting this data prohibit its successful backup. These challenges include limited local technical staff, reliance on manual tape backup processes, and limited WAN bandwidth while the business cannot tolerate data loss or lack of data recovery or productivity in remote and branch operations.

- ☒ **Ensure select data is encrypted.** When firms use removable media that is placed offsite, sensitive data cannot be compromised. Some vertical industries face requirements that specific content, such as credit card and customer data, be encrypted. In these circumstances, technical professionals must implement an encryption approach while managing ease-of-administration, performance, and budget requirements. Some firms are choosing to implement tape encryption, while others seek to eliminate removable media, instead relying upon some form of offsite electronic vaulting. IT management has to properly assess trade-offs in performance and security to determine how and where to encrypt data. For instance, client encryption protects data backup streams at the source and when traveling over the network while adding some performance overhead, whereas media server encryption eliminates both network performance overhead and security while securing the data at rest.
- ☒ **Enable disaster recovery.** Natural as well as human-generated (operator error, sabotage, terrorist attacks) and environmental (equipment, network, power) disasters require disaster recovery planning and capability. Consistent with shortening recovery times, upon a disaster, firms cannot afford days to recover sites, systems, and data. Technology, in combination with policies, procedures, and people, is a key enabler of recovering business operations in the event of a disaster. Challenges with disaster recovery include inefficient or untested disaster recovery plans, time lapses before recovery can be done, and difficulties in recovering the "exact" data protection infrastructure to enable data recovery.

## **BUSINESS CHALLENGES**

Today's backup and storage professionals not only face technical challenges but also must satisfy legal, regulatory, and risk management requirements coming from key departmental stakeholders such as Compliance, Risk Management, Legal, Human Resources, and Records Management officers. In addition, different business units and functional departments such as Engineering, Sales, Marketing, and Finance are requesting improved levels of service in terms of faster rollout of applications supporting a new business initiative, new financial applications, or business intelligence and data warehouse initiatives.

Technical backup and storage professionals must satisfy the following business challenges:

- ☒ **Satisfy recovery SLAs.** Operational recovery for tier 1 and tier 2 applications, on average, must occur in four to six hours. Less critical applications may have recovery times of 8 to 12 hours. For tier 1 through tier 3 applications, it is no longer acceptable for recovery to take days. When a failure does occur, data loss in transaction-oriented systems must be minimized. For these environments, firms require granular recovery points from which to restore. Current backup approaches often prohibit the ability to meet compressing SLAs on recovery.

- ☒ **Support fast rollout of new business applications.** The fast, competitive pace of today's corporate environment requires IT to respond quickly to new opportunities and enable quick deployment of new internal and external business applications as well as rapid upgrades of existing applications. Business units require the ability to quickly address new opportunities by supporting fast rollout of new internal and/or customer-facing applications to meet project schedules and business initiatives. The challenge IT professionals often face is if the IT infrastructure is adaptive enough to meet these business opportunities in the time required.
  
- ☒ **Contain costs.** Today's capex budgets might be incrementally increasing with data, business, and infrastructure growth. However, with corresponding data and storage growth, the opex budgets or the number of administrative resources to manage this increasing capacity is not growing and remains relatively flat. To compensate for this, companies are looking for ways to manage more storage per administrator, which is driving a renewed focus on standardization and ROI in order to get costs under control.
  
- ☒ **Conduct compliance audits.** Firms in many different industries face hundreds of regulatory mandates about how to manage, protect, and retrieve relevant and sensitive content. However, few regulations are very prescriptive, and instead it is the internal policies that drive technology decisions. Data protection — including backup, recovery, and disaster recovery — is central to a sound compliance program. The risk of noncompliance with policy can result in fines, court sanctions, poor publicity, and stock price declines. Legal and regulatory data protection issues bring about the need for companies to:
  - ☐ Provide physical safeguards for specified and sensitive information
  - ☐ Ensure data integrity and protection for specified and sensitive information
  - ☐ Develop and enable business continuity and/or disaster recovery plans
  - ☐ Comply with long-term record retention requirements
  - ☐ Protect data from modification or deletion until the expiration
  - ☐ Enable security of removable media
  
- ☒ **Ensure recovery/business continuity.** Business continuity is a paramount goal to ensure continued business operations, improve competitive position, mitigate regulatory compliance risks, continue processing financial transactions, prevent loss of user productivity, and — ultimately — stay in business during a failure. Business continuity means business productivity and access to applications cannot be compromised or else the result can be transaction loss, delays in time to market, supply chain disruptions, customer loss, cost penalties, and/or regulatory fines. Business continuity is usually satisfied with either clustering and failover services or remote replication, although new approaches such as integrated replication and failover offerings or continuous data protection are being considered.

Many of these technical challenges and business objectives can be achieved by making use of next-generation disk-based data protection to increase performance, improve reliability, shorten recovery times, and eliminate the need to back up redundant data. Given the market dynamics and price declines in disk architectures over the past five years and the proliferation of ATA and SATA disk drives, the use of disk in the data protection path continues to increase.

## **NETBACKUP 6.5 ADDRESSES TECHNICAL AND BUSINESS CHALLENGES**

Symantec Corporation, the undisputed market leader in the data protection and recovery market, has released NetBackup 6.5. The latest version of NetBackup offers an economically viable and rich set of disk-based data protection functions running on an established and proven data protection platform. In the past, disk-based data protection approaches have varied and often been cost prohibitive and/or lacked integration with leading data protection software architectures. Schemas such as backup to disk, disk staging, replication, and the use of virtual tape libraries (VTLs) have proliferated. Recently, newer approaches such as continuous data protection and data deduplication have been evaluated and/or are being deployed. This myriad of approaches has resulted in increased storage administration and cost. Enterprise IT organizations with a plethora of data protection methods in place have expressed their desire for a common and unified data protection framework where different disk-based data protection methods can be centrally managed based on the policies and recovery objectives of each application. Symantec has responded to this market demand with the NetBackup data protection platform, enabling an economically feasible next-generation data protection feature set.

Key disk-based data protection features in the NetBackup 6.5 release are highlighted as follows and are described in detail later in this document:

- ☒ **NEW: NetBackup Enterprise Disk Foundation** features, which are available with all NetBackup Enterprise Disk Options, include the following:
  - ☐ *Intelligent Disk Capacity Management* allows NetBackup to manage a large, shared pool of disks and to optimize both the allocation of disk space and the expiration of backup images, which increases backup reliability and storage utilization.
  - ☐ *Media Server Load Balancing* provides automated and improved load balancing and failover across a pool of shared media servers.
  - ☐ *Storage Lifecycle Policies* allow administrators to create policy templates with different backup and duplication actions, unique media destinations, and varying retention periods for each stage of the lifecycle.

- ☒ **NEW: NetBackup Enterprise Disk Options** are separately licensable options for customers who want to deploy disk-based data protection. In addition to the Enterprise Disk Foundation features described earlier, options include the following:
  - ☐ *NetBackup Flexible Disk Option* provides customers with access to a series of flexible enterprise disk features called AdvancedDisk and SharedDisk. With these features, NetBackup simplifies the management and use of disk for backup and recovery by placing disk volumes or storage arrays into disk pools that can enable reliable, high-performance backup and recovery.
  - ☐ *NetBackup PureDisk Deduplication Option* enables existing NetBackup clients to leverage the advantage of the PureDisk deduplication and replication capabilities. With this option, the NetBackup media server deduplicates data sent to it, also known as target-side deduplication, and then sends the unique data segments to a PureDisk storage pool (requires PureDisk 6.5).
  - ☐ *NetBackup Virtual Tape Library Option* supports NetBackup integration with third-party virtual tape libraries from 17 different vendors and includes a new capability called VTL-direct-to-tape, which allows NetBackup to initiate a duplication to physical tape (or another VTL) directly attached to the VTL and to catalog all copies of data.
  - ☐ *NetBackup OpenStorage Disk Option* supports NetBackup integration with third-party intelligent disk appliances such as those provided by Data Domain, Copan Systems, Sepaton, Diligent, EMC, Network Appliance (NetApp), Quantum, and FalconStor via the NetBackup OpenStorage API. This option allows NetBackup to see the disk on these devices as native disk and to better manage the backup and recovery of data from these devices.
- ☒ **NEW: NetBackup SAN Client** is a new NetBackup lightweight client that sends backups directly over the Fibre Channel SAN using SCSI protocols versus sending the data over a LAN using TCP/IP network protocols. For a single backup stream, this offers up to 150MBps when using disk as a target.
- ☒ **NetBackup Snapshot Client (formerly Advanced Client)** has been enhanced to support new snapshot methods. The new third-party snapshots supported include snapshots from EMC CLARiiON, HP, IBM, and Network Appliance.

Other major enhancements in the NetBackup 6.5 release are highlighted in the following list and are described in detail later in this document:

- ☒ **NEW: NetBackup for VMware and VMware Granular Recovery** provides NetBackup support for the VMware Consolidated Backup (VCB) capability. This allows for backup and restore of Windows and Linux virtual machines while offloading the backup processing from the virtual machines to a third-party or proxy NetBackup server. NetBackup expands upon the VCB integration to enable image-level and file-level restore from a single VMDK backup through offline indexing of the image-level backup with NetBackup FlashBackup technology. This unique feature is now integrated into the NetBackup Enterprise Client.

- ☒ **NetBackup Bare Metal Recovery (BMR)** enhancements include support for Windows network boots, eliminating dependency on local media and offering fast restore for Windows systems in under 15 minutes. Additionally, more platforms have been added for BMR support, including support for Solaris 10, AIX 5.3, Red Hat 4, and SuSE 9. BMR, no longer a separately licensed product, is now part of the NetBackup Standard Client.
- ☒ **NetBackup Encryption:** Customers can choose client- or media server-based encryption. The client encryption feature is now included with the NetBackup Standard Client (no longer a separately licensed option). The Media Server Encryption Option (MSEO) enables encryption of data at rest while avoiding the performance and management implications of client-based encryption. MSEO encrypts data written to tape and centralizes key management on the NetBackup master server.

---

## **NetBackup Enterprise Disk Foundation Features**

To aid customers using disk in the data protection path, NetBackup 6.5 provides a series of Enterprise Disk Foundation features that are included with all the Enterprise Disk Options. These Enterprise Disk Foundation features include Intelligent Disk Capacity Management, Media Server Load Balancing, and Storage Lifecycle Policies and are described in the following sections.

### ***Intelligent Disk Capacity Management***

This feature allows NetBackup to better manage a large, shared disk pool by optimizing disk space and ensuring data is deleted based upon the importance of data.

At the start of a backup to disk, NetBackup estimates the size of the backup job based upon past job history and selects an appropriate disk volume from a pool of disks. Before a backup begins, disk space is preallocated to ensure that it isn't being used by another backup process. Selection of an ideal volume size allows for a backup to be contained within a volume, thus improving backup performance. However, for backups bigger than the largest available volume, a feature called disk spanning allows a job to span multiple volumes in the shared disk pool, thus improving reliability. Finally, NetBackup mounts the assigned volume to the least busy media server (part of the Media Server Load Balancing feature), which helps to improve the speed of backup operations.

The Intelligent Disk Capacity Management feature also improves how NetBackup manages the expiration of backup images on disk. Instead of simply using a "first-in, first-out" approach to delete expired images, NetBackup can expire data based on user-assigned data classification (e.g., bronze, silver, or gold Storage Lifecycle Policies). Thus, if a disk gets full, bronze data will be deleted before silver in order to make room for another backup. This allows customers to improve the possibility of disk-based recovery, even after a backup image may have been moved to tape.

Benefits of the Intelligent Disk Capacity Management feature include the following:

- ☒ Optimizes storage utilization by maximizing use of available space in a pool of disks
- ☒ Improves backup performance because the job is tuned for the right volume size
- ☒ Enhances reliability by mitigating the risk of inadequate volume space

### ***Media Server Load Balancing***

Working in conjunction with the Intelligent Disk Capacity Management feature, the Media Server Load Balancing feature provides automated load balancing and failover across a pool of NetBackup media servers.

With the new Media Server Load Balancing feature, the media server layer is completely virtualized, providing a loosely coupled HA architecture. When a backup job begins, Media Server Load Balancing accesses the "least busy" media server based on CPU, memory, and number of active jobs. Moreover, if one or multiple media servers fail, new jobs are sent only to functional servers and in-progress jobs can be checkpointed and automatically restarted on another available media server(s) in the pool. With this feature, client backups are sent to the least utilized or busy media server, thus optimizing resource utilization and improving completion times.

Benefits of the Media Server Load Balancing feature include the following:

- ☒ Optimizes utilization of existing media servers for improved backup availability and mitigates additional spending
- ☒ Provides high availability, automatically allocating jobs to available media servers
- ☒ Shortens backup completion times by load balancing jobs across media servers
- ☒ Improves reliability by increasing the number of media servers available to receive failed-over backup client jobs

### ***Storage Lifecycle Policies***

An augmentation to the existing NetBackup backup policies, Storage Lifecycle Policies are administrator-defined rules that control the retention periods and location of protected data during its lifecycle, from creation to expiration. A Storage Lifecycle Policy defines one or more storage unit destinations, an action to perform (backup, duplication), the retention type (fixed, capacity based, or expire after duplication), and the retention period for each copy of the data. Storage Lifecycle Policies not only provide backup image copy management but do so intelligently based upon the importance of data so that data can be treated differently based upon its importance to the business. After a backup completes, the Storage Lifecycle Policy initiates image duplications automatically as disk or tape resources become available, queuing or retrying the operation as necessary to ensure that all copies are successfully created. In addition, multiple Storage Lifecycle Policies can share a single disk storage unit, allowing the administrator even further granularity and control.



Benefits of the Storage Lifecycle Policy feature include the following:

- ☒ Meets SLA commitments: ensures data is stored in the right place for the right time
- ☒ Reduces storage costs: stores important data on disk and less important data on tape
- ☒ Reduces risk: ensures data is migrated to tape before deleting from disk
- ☒ Reduces administrative cost: automates data management with lifecycle policies

---

## **NetBackup Enterprise Disk Options**

Tape continues to be a key component in backup operations, although increasingly disk is being used as a complement to improve recovery time objectives (RTOs) and recovery point objectives (RPOs) or to improve reliability or disaster recovery. In addition to the Enterprise Disk Foundation features available with any of the options, the Enterprise Disk Options make backup and recovery faster, more reliable, and more secure. These options provide users with a choice of back-end disk architectures — whether DAS, NAS, SAN, or intelligent disk devices such as OpenStorage or a virtual tape library. These Enterprise Disk Options are described in the following sections.

### ***NetBackup Flexible Disk Option***

The Flexible Disk Option consists of two separate features: AdvancedDisk and SharedDisk. AdvancedDisk is a collection of dedicated disk (DAS, SAN, or NAS) that enables the sharing of file systems across multiple NetBackup disk storage units (DSUs). One of the key benefits is that AdvancedDisk can leverage Enterprise Disk Foundation features such as Storage Lifecycle Policies. SharedDisk allows disks within a disk pool to be shared between multiple media servers of the same platform. This improves the utilization of NetBackup resources and increases the reliability, scalability, and performance of the NetBackup infrastructure.

The Flexible Disk Option delivers two key functions:

- ☒ The ability to share a very large pool of disk (1,000s of TBs) between multiple media servers
- ☒ High-speed SAN backup when paired with the SAN Client

The NetBackup Flexible Disk Option includes the following capabilities:

- ☒ Multiple media servers and Fibre Channel SAN-connected disk volumes are associated in a disk pool. Within the disk pool, volumes are shared dynamically among media servers.
- ☒ Disk LUNs are collectively managed as volumes within a disk pool and shared between multiple media servers for improved utilization.

- ☒ Each volume is dynamically accessible from any media server supporting Media Server Load Balancing and failover.
- ☒ Capacity and performance scale horizontally across all backup clients by adding media servers or storage as needed.
- ☒ DAS, NAS, and SAN configurations are supported. Supported disk targets include qualified storage subsystems from EMC, HDS, Network Appliance, HP, IBM, and Sun.
- ☒ Additional backup performance can be achieved by utilizing the new NetBackup SAN Client.

### ***NetBackup PureDisk Deduplication Option***

The NetBackup PureDisk Deduplication Option is ideal for environments that face growing volumes of data and require an electronic means of providing disaster recovery. To address data growth, the PureDisk Deduplication Option reduces all backup data coming through a traditional NetBackup media server to its possible footprint by leveraging the PureDisk global deduplication technology.

Data deduplication reduces the amount of network bandwidth and storage media required for backup copies because PureDisk writes only one copy of each unique file segment to disk storage. Administrators can configure a NetBackup media server to use a PureDisk storage pool as a NetBackup storage unit, taking advantage of the data deduplication feature of PureDisk. Multiple media servers can share a common PureDisk storage pool, and backup data can be replicated to a second PureDisk environment in a remote datacenter as directed by Storage Lifecycle Policies. The same PureDisk storage pool can be used to serve both remote office backups from PureDisk clients and datacenter backups from NetBackup clients.

The NetBackup PureDisk Deduplication Option enables the following:

- ☒ Existing NetBackup clients and media servers can send backups to a NetBackup PureDisk target.
- ☒ Replication from a local PureDisk pool to a remote PureDisk pool for disaster recovery of NetBackup data.
- ☒ A scalable deduplication storage system with 100s of terabytes of disk and petabytes of backup data.
- ☒ Deployment of an open, data deduplication storage system (for backups) using any combination of arrays and servers.
- ☒ PureDisk works with any storage device, SAN, NAS, DAS, iSCSI, providing cost-effective and ultimately scalable options for data storage.

### ***NetBackup OpenStorage Disk Option***

The NetBackup OpenStorage Disk Option is suited for firms that want to leverage third-party commercially available intelligent disk appliances. As virtual tape libraries and other intelligent appliances continue to improve and add extended functionality for data protection, deduplication, and replication, this broader feature set can be centrally managed by NetBackup as an OpenStorage integrated device. This OpenStorage integration is enabled through a new API from Symantec that is used to enable direct integration between NetBackup and new types of third-party intelligent disk appliances such as VTLs and deduplication appliances. The intelligent disk appliance supplier develops a NetBackup plug-in that is installed on the NetBackup media server, and Symantec works with the vendors to jointly test and qualify the solution. The OpenStorage integration provides a single, consistent approach for NetBackup to write to intelligent disk appliances as disk. NetBackup sees the devices as native disk. This allows NetBackup to take advantage of the speed and capacity of disk, the extended functionality with the appliances, and all the Enterprise Disk Foundation features (e.g., Storage Lifecycle Policies). In this manner, customers gain easier access to data on these devices and the ability to control functions like replication and duplication. OpenStorage ensures deep integration and management of intelligent disk appliances for NetBackup customers who prefer the appliance's ease of use and value proposition.

The NetBackup OpenStorage Disk Option enables the following:

- Centralized point of control for management and recovery of data written to intelligent disk devices
- Flexibility to manage backups across intelligent storage devices from different companies

### ***NetBackup Virtual Tape Library Option***

The NetBackup Virtual Tape Library Option supports NetBackup integration with third-party virtual tape libraries from 17 different vendors and includes a new capability to initiate physical tape copies from virtual tape copies along with full cataloging of all those copies.

The NetBackup VTL direct-to-tape feature, which addresses previous challenges in creating physical tape copies of virtual tape backups. Prior to this feature, there were two means of creating physical tape copies: use the NetBackup tape duplication or rely on the VTL to make physical tape copies. Using NetBackup duplication routes data through the NetBackup media server and creates overhead and resource consumption and is like performing two backups — to the VTL disk and then to tape. Using the VTL capability keeps the input/output load off the media server, but the physical tape copy is not cataloged by NetBackup, resulting in more complex, two-step restores and a nonsupported usage model. With this feature, NetBackup manages the duplication of backup images, enabling the VTL to move the data from virtual tape to physical tape (or another virtual tape) under NetBackup control. This results in NetBackup cataloging the duplications so that restores can be activated from virtual or physical tape as needed.

---

## **NetBackup SAN Client**

Prior to NetBackup 6.5, the only way to perform high-speed backups over the SAN was with the SAN Media Server. SAN Media Servers are most often used to do high-speed backups to shared, SAN-connected tape drives. The SAN Media Server requires installation of a full Media Server on the application server. It is possible to back up to disk targets with SAN Media Server, but the disk storage units (DSUs) must be dedicated to the SAN Media Server, so 50 SAN Media Servers would require 50 DSUs to create and administer.

New in NetBackup 6.5, the SAN Client, included as part of the NetBackup Enterprise Client, allows high-speed backups to shared disk resources. Instead of sending I/O directly to the target storage, SAN Client sends data to a new class of media server, which then writes the streams to shared media server-connected disk. The new media server architecture involves a front-end HBA to which the SAN Client connects and a back-end HBA, which connects to the shared disk resource.

In the first release of the SAN Client, this front-end HBA must be a qualified QLogic HBA because a special target-mode driver has to be written for it (although the "back-end" media server HBA can be from any vendor). The performance design goal for the SAN Client is up to 150MBps per stream, but a single client can support multiple streams, meaning that even faster multistream performance can be achieved. The design goal for the target-mode driver is upwards of 500MBps aggregate per media server, which is on the order of five times faster than traditional LAN backup.

The NetBackup SAN Client, which is part of the NetBackup Enterprise client, can leverage new disk features and options (e.g., OpenStorage and Flexible Disk). Key benefits of the SAN Client include the following:

- Faster backup operations for Windows, Solaris, Linux, HP-UX, and AIX clients with SAN attached storage
- Lower CPU and memory requirements for backup operations when compared with the SAN Media Server

---

## **NetBackup Snapshot Client**

The NetBackup Snapshot Client provides integration with Symantec snapshot technologies or array-based snapshots, allowing administrators to select and leverage third-party point-in-time copies for backup and restore operations. One of the primary benefits of the NetBackup Snapshot Client is the ability to move I/O processing from the primary NetBackup client to a backup agent, thus offloading processing from the applications server and allowing for backup to be done in the background.

Another key benefit to snapshot methods is the ability to recover data more quickly in the event of a failure or data corruption significantly improving RTOs and, possibly, RPOs. NetBackup supports different snapshot methods for file systems, applications (such as SAP and Exchange), and databases. NetBackup also offers customers unique features such as FlashBackup — the ability to quickly back up millions of files (using a raw-partition backup approach) and then easily recover an individual file — and Instant Recovery — the ability to restore deleted files in seconds (especially when performing frequent snapshots).

With NetBackup 6.5, enhancements have been added to Snapshot Client to provide the following:

- ☒ Allow NetBackup to manage and control snapshots of file systems and applications using NAS storage (currently NetApp only) including Windows, Solaris, and Linux systems, and SAP and Oracle on Solaris systems
- ☒ Manage protection and recovery of Microsoft Exchange data on NetApp storage
- ☒ Schedule and manage new third-party snapshot methods on arrays including EMC CLARiiON (e.g., SnapView Clone or SnapView Snapshot) and HP StorageWorks Enterprise Virtual Array (EVA)
- ☒ Protect and recover more Unix and Linux data with expanded support for local and alternate client backup methods and Instant Recovery
- ☒ Expanded VSS snapshot support on EMC Symmetrix/DMX, HP StorageWorks EVA, and NetApp NAS devices
- ☒ Instant Recovery feature for clients using the VSS snapshot method on new selection of arrays (The Snapshot Client/Array Compatibility List found at <http://support.veritas.com/docs/279042> provides more details.)

Because of the large number of variations around platform and application support for snapshot methods, it is impractical to list the broad range platforms and methods supported by NetBackup. For customers interested in leveraging snapshot methods for faster backup and recovery, NetBackup can help centralize and simplify the use of snapshots for faster data recovery.

---

## **NetBackup for VMware**

Server virtualization has moved beyond test and development to production environments. Virtual servers are ideal for consolidation and improved mobility, but they require protection. The most common approaches to protecting virtual environments are installing a backup client on each virtual machine or backing up the VMDK files directly off shared SAN storage. With a client-on-each-VM approach, processing overhead is high. However, by installing a PureDisk client in the VMware virtual machines, PureDisk's data reduction abilities make client backup feasible for many VMware environments.

NetBackup for VMware extends the means of protecting VMware environments by utilizing the VMware Consolidated Backup (VCB) framework. This isn't unique, as other vendors also offer VCB support. What is unique with NetBackup 6.5 is it enables users to perform two types of restores, either individual file-level Granular Restore or the entire VMDK image with a single backup pass. The Granular Restore feature allows for backup at the VMDK level but also maps, catalogs, and backs up the individual files. This patent-pending feature leverages the NetBackup FlashBackup mapping capability to take the snapshot backup and map it to allow for a single-file or full snapshot recovery. Other vendors require two backup passes to offer the same level of support, which means double the network I/O and double the storage.

## Other NetBackup 6.5 Features

In addition to the features and options previously described, NetBackup 6.5 offers the following enhancements and capabilities:

- ☒ Enhancements to the **NetBackup Bare Metal Recovery** feature include bundled support for Windows network boots, via NetBackup Standard Client, eliminating dependency on local media and offering fast restore for Windows systems in under 15 minutes. Additionally, more platforms have been added for BMR support, including support for Solaris 10, AIX 5.3, Red Hat 4, and SuSE 9.
- ☒ Support for **new NetBackup client and server platforms** is included. The following support has been added: Solaris 10 x64 64-bit server and client support; Windows Vista client support; ACLS support for Macintosh, Linux, and Solaris 10 ZFS clients; and Novell OES NSS support for the SuSE client.
- ☒ The **tape media sharing** feature allows multiple NetBackup media servers to actively share a given tape media for write purposes. Media sharing reduces tape media-related expenses by enabling increased media utilization, which in turn reduces the amounts of partially full media and total number of tape media required to store a given amount of backup data. Media sharing reduces the vaulting-related expenses because fewer pieces of media will need to be vaulted and fewer pieces of empty media will need to be placed into the scratch pool. Media sharing also provides the ability to "hand off" a mounted tape to another media server, eliminating mount time for backup to different media servers.
- ☒ **NetBackup LiveUpdate** includes a LiveUpdate agent option that enables customers to download and install patches for NetBackup, NetBackup add-on products, and PBX. Only NetBackup versions 6.5 and later can be used with NetBackup LiveUpdate. NetBackup LiveUpdate features include the following:
  - ☐ Patches can be downloaded for both Windows and Unix platforms.
  - ☐ Downloaded patches can be installed remotely to NetBackup servers and clients.
  - ☐ Cross-platform installation of patches is supported for both Windows and Unix.
  - ☐ Patches can be downloaded and installed on Unix clustered systems.
  - ☐ Administrator privileges are not required for patch installation on NetBackup servers and clients.

NetBackup LiveUpdate is an additional method to obtain patches quickly and more conveniently. The current program for customers to obtain patches remains in place.

## **ONGOING DATA PROTECTION CHALLENGES**

The manner in which backup copies of primary data are created has been changing over the past 10 years. Convergence between traditional backup to tape and the use of disk for disk staging, replication, and archiving has occurred. And now new technologies such as data deduplication and CDP are emerging. This technology convergence has resulted in different technologies, architectures, and administration models. Users want to be able to take advantage of new technologies while they leverage existing applications and avoid the need to rip and replace products. IT organizations need to be able to select the right technology to meet different application requirements based on RTOs and RPOs. Administrators seek to manage different data protection workloads from a common platform with centralized management. From a cost-of-ownership perspective, budgets require flexibility in back-end disk architectures to avoid increased administration in disparate architectures and capital costs in storage redundancy. As a result of these market and technology dynamics, some fundamental challenges still exist. These challenges are noted in the following sections.

---

### **Backup Versus Archive**

Many firms still rely on backup technology to perform archiving for long-term retention of electronic records. And much confusion exists in the market between backup and archive. However, backup and archive software workloads serve different use cases. Commonly, backups are overwritten as new, more recent backups are created. Archiving is used for the purposes of long-term retention, preservation in the event of a legal discovery, or general IT storage, performance, and backup window optimization. At the root of these different approaches is content indexing. A software-based archiving process performs a full-content indexing of the files or messages that it is archiving. Thus, users can conduct a keyword search and retrieve only files related to the search. Conversely, backups do not have this native capability and a restore must be performed of a backup image before more granular searching can be conducted. Over time, new technology integration will enable these different workloads to converge, but today these processes remain standalone. Symantec provides integration between NetBackup and Enterprise Vault for the use cases of data migration, data recall, and policy. In the first use case, Enterprise Vault archive files can be collected and migrated into NetBackup in the event of a failure. In the second use case, a NetBackup retention can be set to infinity so that Enterprise Vault controls the automatic migration and seamless data recall. Lastly, a policy name in Enterprise Vault policy manager matching a backup policy name in NetBackup allows for consistent archiving, collection, migration, and retention.

---

### **Legacy Data, Formats, and Media**

Most large enterprises have multiple backup applications and architectures in place. Although this approach is not ideal from an economic or administrative perspective, the challenge of eliminating the disparate infrastructures is often the obscure or unexpected need to restore older data from legacy applications, created in a legacy format on a legacy piece of media. Often IT organizations need to keep older systems, software, and hardware in place to support the restore or recovery of data on an old tape. This persistence in data, formats, and technology can often run

at odds with allowing firms to migrate to next-generation data protection products and architectures. The manner in which most backup applications address this is by supporting the storage of data in a standard Unix tar format, which mitigates the legacy data and format issue.

---

## **Disparate, Distributed Data Protection Technologies**

IT organizations are placing increasing focus not only on data within controlled datacenter environments but also on data in remote and branch offices. This distributed data in hundreds to thousands of remote locations has commonly been undermanaged. Firms with existing, resource-limited, costly, or unreliable remote office backup are shifting to centrally managed and controlled WAN-based data protection approaches to satisfy business requirements and meet the demands of increasingly stringent business unit SLAs. Capacity-optimized, disk-based enterprise remote office data protection solutions are emerging — in response to the increasing need for cost-effective, centralized control of enterprise remote office data availability, recovery, and administration — to address the historical enterprise remote office data protection challenges that have included limited to no technical staff onsite and insufficient network bandwidth. Expensive, redundant backup processes at each remote office location create islands of disparate hardware, software, data, and resources — all managed separately and outside the control of a centralized IT policy.

## **CONCLUSION**

Because of current business drivers and the technology landscape, firms are using more disk in the data protection path. There are many different options for firms to choose from to improve reliability, recovery, and performance. The challenge is how to implement disk to achieve operational and business policy improvements without disrupting existing users, applications, and infrastructure. Today, users of NetBackup environments can upgrade to unparalleled disk-based data protection features to improve operational recovery, increase backup-and-restore reliability, and optimize SAN-based backup performance while leveraging the back-end disk architecture of their choice. NetBackup 6.5 solves business and technical challenges around data protection and provides the underlying data protection platform of the future. For customers who have different application-level SLAs around data protection and recovery, the NetBackup platform provides centralized management of heterogeneous or disparate data protection technologies, and with the full proliferation of virtualized servers out there now, NetBackup offers a market-leading solution for VMware environments.

---

## **Copyright Notice**

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2007 IDC. Reproduction without written permission is completely forbidden.