Delivering a New Level of Data Protection Resiliency with Appliances

Who should read this paper

- Directors of IT and IT Managers
- Backup Administrators and Architects
<table>
<thead>
<tr>
<th>Content</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Data integrity</td>
<td>1</td>
</tr>
<tr>
<td>Threat protection</td>
<td>1</td>
</tr>
<tr>
<td>Redundant architecture</td>
<td>2</td>
</tr>
<tr>
<td>Environmental and operational efficiency</td>
<td>3</td>
</tr>
<tr>
<td>Symantec NetBackup Product Family</td>
<td>3</td>
</tr>
<tr>
<td>Summary</td>
<td>6</td>
</tr>
</tbody>
</table>
Introduction

When it comes to backup and recovery as well as a host of other applications, your always-on enterprise demands resiliency. The consequences of downtime can be costly – ranging from lost or deferred revenue to a damaged reputation and reduced confidence in the IT team’s abilities.¹

There is no such thing as a “good time” for downtime, which means your organization needs to consistently re-visit its approach to achieving high availability in order to keep your business running 24/7/365 and meet the demands of your employees as well as customers.

This solution brief examines four (4) critical areas to focus on when it comes to achieving resiliency with Purpose-Built Backup Appliances (PBBAs)³:

- Data integrity
- Threat protection
- Redundant architecture
- Environmental and operational efficiency

These four (4) areas are key contributors to helping your organization minimize its downtime and ensure recovery whenever and wherever it is needed.

Data integrity

Protecting system data and its integrity ensures your data is recoverable if corruption occurs. When evaluating data integrity capabilities in a backup appliance, you should be certain that key data integrity features are integrated into the system, including:

- **Pre-set backup policies**: The appliance should come pre-set with backup policies to automatically protect existing and new deduplication storage pools as well as those already configured on a prior appliance.

- **Automated shadow copy creation**: The appliance should be able to automatically create daily shadow copies of system data to ensure integrity. It should also have auto-detection for corruption and be able to perform a restore from the most recent shadow copy.

*The bottom line: The appliance should help you reduce your setup and administration time, while guarding against human error that can occur when automatic backup policies and shadow copy creation are not in place for preserving data integrity.*

Threat protection

The backup appliance should offer built-in, policy-based protection that helps secure servers using host-based intrusion prevention (i.e., Intrusion Prevention System – IPS) and detection technology (i.e., Intrusion Detection System – IDS). The security solution should be able to monitor and act on “normal state” without using signatures or requiring continually-updated content.

³ Purpose-Built Backup Appliance integrated system is defined by IDC as tightly integrated with backup software are called PBBA integrated systems. PBBA integrated systems can have master or media servers integrated into the system to orchestrate the backup and movement of data to other systems or removable media such as tape. (e.g., Symantec NetBackup 5200 and 5300 series appliances).


Below are two (2) examples of what this technology should do for you:

- **IPS**: Allows you to set an intrusion prevention policy to prohibit unauthorized users or applications from accessing backed up data.
- **IDS**: Acts as a detection engine that monitors significant system events and critical configuration changes in real-time, including user logins, logouts and failed log on attempts.

The bottom line: **The appliance must feature built-in threat protection from an industry-leader in security.**

**Redundant architecture**

System availability starts with the design of the appliance. It must be architected with both proactive and reactive controls to maximize redundancy and availability.

**Proactive**

The appliance should offer multiple redundant data paths from node to storage so that it is able to withstand multiple component failures and still operate. It’s also important to have dual components with dual pathing on all critical storage (e.g., FC HBA, RAID controllers and disk drives). This configuration will deliver greater protection and system availability. Ideally, the dual RAID controllers should be external. For additional redundancy, the following components should be hot-swappable:

- RAID and disk-controllers
- Power supplies
- Fan modules
- Disks

When aiming to achieve resiliency with an appliance, it is important to have fully automated monitoring in place for hardware components to help minimize downtime. The system should have the built-in ability to notify the appliance vendor’s support team as well as the backup administrator of any possible issues or problems - before they cause downtime.

Built-in disaster recovery for the deduplication engine is another critical piece to ensuring system redundancy. The integrated appliance should offer fast, resource-efficient and reliable deduplication performance. It should give you fast restore performance, ensure data integrity for the deduplication storage system, provide protection in case of catalog failure and allow for automatic recovery from either the real-time catalog shadow copy or crash-consistent recovery from tape backup.

**Reactive**

One of the key benefits of an appliance is that it gives you the ability to go through a single vendor for all of your support needs. Make sure that the appliance you are evaluating is in fact built and supported by a single vendor that offers built-in support functionality (often referred to as auto-support) and reactive monitoring capabilities.

The bottom line: **The appliance should help you reach your goal of higher availability with lower total cost of ownership by giving you capabilities to proactively identify issues, automate support case management and resolve issues more quickly, while maximizing redundancy and availability.**
Environmental and operational efficiency

With an appliance, you should not have to sacrifice environmental and operational efficiency in order to achieve resiliency and redundancy. In fact, it should be just the opposite. Moving to a fully integrated backup appliance should offer you increased environmental efficiencies, driving IT productivity and enabling business agility.

The right integrated backup appliance should offer redundancy and resiliency, while allowing your organization to:

- Reclaim precious data center rack space
- Reduce power consumption
- Reduce cooling consumption

_The bottom line: The appliance should help you increase environmental efficiencies by allowing you to reallocate your critical data center infrastructure resources to new IT investments. It should also help you achieve operational efficiencies by streamlining and eliminating manual processes thus reducing the potential for human error._

Symantec NetBackup Product Family

Symantec NetBackup is a market-leading backup and recovery solution for critical IT resources. The NetBackup family includes both the NetBackup 5230 and 5330 appliances; integrated backup appliances delivering performance, scalability and resiliency.

The NetBackup 5330 and 5230 are complementary products and form a product family. Each appliance addresses different customer needs based on performance, capacity, resiliency, and price. The NetBackup 5330 appliance is designed as a media server with storage capacity and is optimized for performance and resiliency. Alternatively, the cost-optimized NetBackup 5230 is multifunctional—from master, media, or combination server, to an integrated appliance with deduplication.
Take your organization to the next level of data protection resiliency with Symantec backup appliances

Data Integrity

The NetBackup 5230 and 5330 appliances help reduce your setup and administration time, while guarding against the human error that can occur when automatic backup policies and shadow copy creation are not in place for preserving data integrity.

The NetBackup 5230 and 5330 allow you to automatically create a backup policy for system data when:

- A new deduplication storage pool is created during the initial configuration of the appliance
- A new deduplication storage pool is created that did not previously exist
- Upgrading an appliance that had a deduplication storage pool already configured

They can also automatically create daily shadow copies of system data. In addition, the NetBackup 5230 and 5330 can detect corruption in any part of the system and automatically perform a restore from the most recent shadow copy (with zero downtime). They are also configured to reduce disk space consumption and deliver faster file system recovery in the event of a crash.

- **Data integrity for the deduplication storage system:** The NetBackup 5230 and 5330 deduplication architecture allows any unrecoverable portions to be immediately isolated from the rest of the functioning data in the deduplication storage system. This capability marks unrecoverable segments for deletion and ejects them from the deduplication storage system. Since duplicate data can continue to be referred to repeatedly for any future backup jobs, compromised data isolation is critical for the deduplication storage system. If compromised segments are continuously referenced, data corruption can continue to spread within the deduplication pool, further worsening the impact of the corruption. To prevent this, the NetBackup 5230 and 5330 feature a warning system that automatically alerts your system administrator of this occurrence and provides detailed remediation steps so they can repopulate the deduplication storage system with any compromised data. This functionality is critical to increasing the robustness of your storage system and making it continuously functional - even when a portion of it is compromised.

- **Catalog integrity for the deduplication pool:** The NetBackup 5230 and 5330 appliances perform online data integrity checks of all catalog objects, reference count objects and data store objects. They also check all the internal pointers and references between them since any missing objects or pointers may indicate compromised data. The online integrity check runs as a background maintenance task so it does not impact data protection activities, including backups, restores and deduplication updates to the deduplication storage system. Separating maintenance tasks and data protection tasks means data integrity checks can be run simultaneously with data protection tasks - without jeopardizing performance. The NetBackup 5230 and 5330 also have controls in place to ensure that data contained in the deduplication storage system has not been unintentionally altered or corrupted in any way. In most cases, the online data integrity check should self-correct any issues it finds. If an unrecoverable issue is detected, the NetBackup 5230 and 5330 warning system automatically alerts your system administrator to which backup point-in-time, client and policy is affected and suggests immediate remediation steps. These steps help your administrator adequately re-populate the corrupted portions of the deduplication storage and restore any previously unrecoverable data.

Threat Protection

Symantec Critical System Protection (CSP) software is built into the NetBackup 5230 and 5330 appliance software. This industry-leading protection goes deep on delivering Intrusion Prevention Services (IPS) and Intrusion Detection Services (IDS) as a fully integrated feature of the appliance:
Intrusion Prevention (IPS) | Intrusion Detection (IDS)
---|---
- Real-time proactive enforcement
- Intrusion/malware prevention
- OS hardening
- Application control
- Privileged user access control
- Vulnerability & patch mitigation
- Real-time monitoring/auditing
- Host intrusion detection
- File integrity monitoring
- Configuration monitoring
- Tracking/monitoring user access
- Logging
- Event reporting

**Redundant architecture**

The redundant architecture of the NetBackup 5330 differentiates it from other integrated appliances available today. Significant enhancements have been made to the architecture to provide advanced storage and hardware protection:

- Multiple data paths between compute node and storage mean the NetBackup 5330 can withstand multiple component failures and still operate.
- Dual components with dual pathing on all critical storage (including Fibre Channel (FC) Host Bus Adapter (HBA), RAID controllers and disk drives).
- Redundant hot swap components, including RAID and disk controllers, power supplies, fan modules and disks provide additional redundancy and also make it easy to pull out parts and replace them in the event of an issue.
- RAID controller backup-battery ensures data integrity is maintained (and corruption prevented) in the event of a power failure.
- RAID6 layout allows for two (2) concurrent drives in either failure or rebuild mode, providing faster RAID rebuild times. The NetBackup 5330 also provides a hot spare for every RAID set that automatically takes the place of a failed drive.
- Network and fibre channel redundancy via a number of fibre channel and gigabyte Ethernet I/O configurations.

The NetBackup 5230 and 5330 help you reach your goal of higher availability with lower total cost of ownership by giving you capabilities to proactively identify issues, automate support case management and resolve issues more quickly, while maximizing redundancy and availability.

**Environmental and operational efficiency**

**Environmental efficiency:** The NetBackup 5330 is the only integrated, purpose-built appliance to earn the Energy Star certification. Not only does the appliance reduce power and cooling expenses compared to other backup appliances, but it has great density, which means it delivers more terabytes of usable capacity per rack space unit (RSU), or floor space, than competing products.

**Operational efficiency:** The NetBackup 5230 and 5330 feature centralized administration with wizards for configuration and policy creation, single software patch and firmware updates and a single support contact (i.e., a single vendor for support vs. multiple OEMs), eliminating the need for manual processes and reducing the potential for human error.
The bottom line: We recommend that you look for these capabilities in an integrated backup appliance:

1. End-to-end data integrity for all parts of the storage system
2. Built-in protection (prevention and detection) from security threats
3. Architecture designed specifically for redundancy
4. Environmental and operational efficiency

**Confidence with NetBackup Appliances**

NetBackup Appliances give you the confidence that your data is fully protected against disaster. We know our appliances are the “last line of defense” for making sure you can recover your data and files when you need it and without disrupting your organization’s operations, even when unexpected events occur.

NetBackup Appliances tightly integrate NetBackup data protection software with a highly optimized hardware platform. NetBackup appliance deployment consists of the complete installation and configuration of all appliance components to create a backup environment that is ready to use and delivers a faster return on investment.

**Summary**

Symantec has taken a balanced approach to data integrity, focusing both software and hardware optimized designs that are the benefit of decades of engineering experience. We look at data integrity as an expected attribute of our backup systems rather than a feature. Enterprises can rest assured their information is correct, secure, and accessible when needed.

With NetBackup appliances, Symantec delivers resiliency by ensuring key functionality is built into the appliance that protects the integrity of your valuable data, guards against threats, and increases environmental and operational efficiencies. The ideal appliance should be able to deliver resiliency for your always-on organization, and with a lower overall total cost of ownership (TCO).
About Symantec
Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company’s more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenue of $6.7 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.