TANEJA GROUP
TECHNOLOGY ANALYSTS

SOLUTION PROFILE

Meeting the Top Backup Challenges in Small and Medium Business Environments

December 2008

Although small and medium businesses (SMBs) do not typically generate the same amount of data that large enterprises do, they still require the same kind of reliable protection to ensure timely recovery of critical business data and systems. The limited resources with which many SMBs contend, however, presents a different set of challenges for achieving this level of protection. When evaluating data and system protection solutions, most SMBs look for cost-effective solutions that are easy to use and provide the functionality they need – in that order.

As evolving business and regulatory mandates drive ever more stringent requirements for data backup, restore, and retention, SMBs must plan data and system protection deployments with a comprehensive understanding of the challenges. In this Solution Profile, we'll summarize what we see as the top six challenges SMBs need to consider as they craft comprehensive data and system protection solutions, pointing out the technologies that can be used to address them.

Identifying the Challenges

The base requirement for a protection solution is to provide rapid, reliable, and comprehensive recovery of important systems and data to desired recovery points with minimal impact on business operations. Due to smaller budgets and a lack of widespread storage expertise relative to larger enterprise environments, SMB backup administrators need these solutions to be cost-effective and easy to use as well. Regardless of industry, SMBs face a common set of challenges when implementing and managing a protection strategy:

Implementing comprehensive protection with minimal impact on business operations. Although most SMB environments are Windows-centric, many have at least some critical data on other platforms such as Linux, Unix, or NetWare. Critical data is created on server, desktop, and laptop devices, some of which are often not connected to a network. And increasingly, SMBs are implementing virtual server environments to reap the benefits of higher server utilization and consolidated management. Keeping track of all these data "sources", and identifying new sources as they are brought online so they can be adequately protected, particularly with the proliferation of virtual server images, is problematic.

Gone are the days when critical systems can be shut down to perform backup operations. Explosive data growth rates of 50% or more are forcing all companies, regardless of size, to deal with much greater amounts of data, putting significant strain on existing backup

87 Elm Street, Suite 900 Hopkinton, MA 01748 Tel: 508-435-5040 Fax: 508-435-1530 www.tanejagroup.com

processes. Backup operations need to be as transparent as possible, requiring limited to no end user involvement.

Meeting increasingly more stringent protection requirements in the areas of backup window, recovery point objective (RPO), recovery time objective (RTO), and recovery reliability. Increasingly, SMBs are seeking more efficient ways to reduce or eliminate their backup windows. The requirements to recover lost or corrupt data back to a specific point in time (measured as RPOs) and reduce the overall time to restore data (measured as RTOs) are becoming more stringent and are now often measured in hours instead of days. Due to the increasing criticality of data, recovery reliability is also a point of concern. What is clear is that tape-based backup infrastruc-tures are increasingly unable to meet the challenges in this area by themselves.

Dealing with limited backup administration resources. This issue tends to be a larger concern with smaller companies that may have no dedicated IT staff, or possibly only one admin responsible for all IT operations. Even in larger SMBs, the concept of a dedicated backup admin is a rarity, and very small staffs must contend with protecting data that may be spread across multiple geographical locations and systems, some of which are only sporadically connected to a network (e.g. laptops). Our interaction with end users indicates that a large percentage of critical data is generated by distributed clients, and an inability to protect this data can leave SMBs open to data loss that can have a significant impact on the business.

Deploying disaster recovery (DR) strategies cost-effectively. Because of the complexity associated with setting up and maintaining DR strategies, many SMBs do not have them. They lack the resources, distributed administrative expertise, and off-site storage locations that are required to provide DR capabilities. The legacy practice of backing up to tape and then shipping those tapes to outside contractors like an Iron Mountain for off-site storage can be fraught with risk; end users cannot be relied upon to do this consistently, centralized backup resources may not be aware of critical new systems and data, and there have been a number of disturbing stories in the press about tapes disappearing during shipment or unable to be found when restores are required.

Leveraging new technologies non-disruptively to improve backup and restore operations. With each successive release of protection solutions, new technologies become available, and last year's intractable problem can become next year's non-issue. But SMBs have significant investments in their infrastructure and processes, and for these technologies to help, it must be possible to deploy them non-disruptively.

Maintaining a secure backup and recovery environment. SMBs need to think about this issue in two areas: providing adequate security including encryption and virus protection, plus centralized management of an entire data protection infrastructure, ensuring backup data both in-flight and at-rest is protected and efficiently managed.

87 Elm Street, Suite 900 Hopkinton, MA 01748 Tel: 508-435-5040 Fax: 508-435-1530 www.tanejagroup.com

Matching Solution Technologies

Implementing comprehensive coverage with minimal impact to business operations. Platform coverage can be easily verified as you evaluate protection solutions, so check to make sure the platforms you have are covered. If you have data stored in SAN, NAS, and/or DAS environments, ensure that your backup solution covers them. Look for policy-based backup schedulers that provide an ability to dynamically deal with failed backup jobs or disconnected clients without operator intervention. An ability to back applications up on-line, often through the use of snapshot backup interfaces, can help to minimize business impacts but beware of processing overhead impacts on backup clients. What you're looking for are efficient approaches which can do volume level backups but still provide object-level restores, such as individual files or individual e-mail messages or mailboxes in Exchange environments.

Meeting increasingly stringent backup and recovery requirements. Most products support incremental and differential backup options, both of which can shorten backup windows and lower network bandwidth requirements; ensure, however, that if you plan to use these features that "synthetic full" backups are generated on demand at the time of the restore to simplify recovery operations. By inserting disk into your backup infrastructure, you will shorten backup windows and improve RPO/RTO. Blending disk and tape appropriately in a backup infrastructure, using disk for higher duty cycle tasks such as initial backups and object-level restores from recent backups, and tape for lower duty cycle tasks such as storing older backups or restores of very large data sets (like would be required for DR purposes), you can leverage disk's advantages (random access) and tape's advantages (very low cost storage) together to achieve optimal performance at low cost while improving overall recovery reliability. Continuous data protection (CDP) technology, a disk-based backup approach, transparently captures data throughout the day as it is created instead of all at once during a "backup" and is particularly effective at handling disconnected clients and limited bandwidth environments. Because data is effectively being collected all the time, CDP can provide very granular recovery options, leading to RPO improvements. When data is stored on disk, there is the opportunity to deploy data de-duplication against it to reduce the raw storage capacity required to store a given amount of data. Data de-duplication can lead to data reduction ratios of 20:1 or more over time with no data loss, and by working with data in "capacity optimized" form, SMBs will be transmitting significantly less data across networks, reining in storage capacity growth, and minimizing power, cooling, and floorspace costs associated with disk-based backup infrastructure.

Snapshot backup technologies provide a non-disruptive way to offload backup processing from backup clients while still providing application-consistent recovery points. Look for products that support Microsoft's Volume Shadowcopy Services (VSS) for popular Windows applications like Exchange or SQL Server or VMware Consolidated Backup (VCB) for virtual machine (VM)

87 Elm Street, Suite 900 Hopkinton, MA 01748 Tel: 508-435-5040 Fax: 508-435-1530 www.tanejagroup.com

environments based around VMware. VCB is an example of a backup optimization available in VM environments; instead of backing up at the VM layer, VCB provides a documented interface that allows third party backup products to back data up at the hypervisor layer, and yet still support individual VM and object-level restores. A VCB snapshot can then be offloaded to a backup proxy, which can be either a physical machine or a VM, so that backups have almost no impact on production applications.

Dealing with limited backup administration resources. Centralized management with significant automation is the most effective way to provide a very scalable data protection solution that can be administered with few backup administration resources. Look for solutions that leverage backup to disk to minimize the need for end user involvement and tape handling, even in remote locations and for disconnected clients, but can integrate with tape-based infrastructure at centralized or DR locations for very low cost storage over time.

Deploying DR strategies cost-effectively. Exporting to tape and storing those copies in an off-site location has been the historical approach to DR, but a lack of administrative resources and budget can be real stumbling blocks to DR in SMB environments. Disk-based backup options give you access to replication technologies that can be used to transmit backup data to DR sites more quickly and without having to ship tapes. Backups can then be exported to tape at the DR site. Storage capacity optimization (SCO) technologies such as data de-duplication can be used to significantly decrease the amount of data that needs to be replicated to remote sites, making much better use of available bandwidth. Alternatively, cloud-based backup media target options provide an even simpler solution to the DR problem, providing immediate access to off-site storage for literally pennies per gigabyte. And don't forget support for system-level recoveries (bare metal restores or BMR) that may have to be performed in the event of an unrecoverable server failure. BMR technology provides complete protection (system + data) and can support restoring to dissimilar hardware or virtual environments for increased flexibility. Certain BMR products use disk-based imaging approaches to create bootable images for recovery purposes that include not only system data (applications, operating system, patches and tweaks) but also file-based data, a capability which significantly simplifies and speeds up complete system restores when they are required, regardless of whether restoring to physical or virtual environments. These products can be used in conjunction with pure file-based enterprise backup software, often with schedules that interleave more frequent file-based backups with less frequent imaging-based backups. While SMBs can just use disk-based imaging products for backup purposes, file-based products tend to offer more flexibility by supporting capabilities such as heterogeneous platforms, CDP, advanced application backup, tape-based infrastructure, etc. Disk-based imaging technology can also be very valuable in simplifying server migrations.

Leveraging new technologies non-disruptively. Critical new technologies in the

87 Elm Street, Suite 900 Hopkinton, MA 01748 Tel: 508-435-5040 Fax: 508-435-1530 www.tanejagroup.com

backup arena include disk-based backup targets, application-consistent snapshot backups, disk image-based backups, the use of data de-duplication, CDP, and cloud-based backup targets. The benefits these bring have all been discussed, but it's important to look for data protection solutions that not only incorporate them but allow their use with minimal changes to existing processes.

Maintaining a secure data protection environment. Encryption is the best way to address this issue, and we recommend end users deploy standards-based solutions, such as AES, that are at least 128-bit. To encrypt data in-flight, you'll need an option to encrypt on the source (i.e. the backup client) before the data is sent across the network, but understand that encryption will generate overhead so be sure that source-based options do not result in unacceptable backup performance impacts. Target-based encryption options exist as well but leave data unprotected as it travels between the backup source and target. Finally, ensure that backup management consoles are at a minimum password-protected, and so much the better if they support multiple levels of secure access.

Taneja Group Opinion

SMB environments may not need the scale provided by enterprise-class backup and recovery solutions, but they need much of the same functionality. Policy-based backups, automated operations, and centralized management are key design tenets to help lightly staffed SMBs effectively manage system and data protection operations. Integrated DR capabilities make it easy to rapidly restore complete systems. Newer technologies like disk-based backup, application-consistent snapshot backups, disk image-based backups, the use of data de-duplication, CDP, and cloud-based backup options will help SMBs address shrinking backup windows, increasingly stringent RPO/RTOs, and recovery reliability concerns. End users should demand this functionality from data and system protection solutions that can be deployed non-disruptively and also meet their cost and ease-of-use requirements.

87 Elm Street, Suite 900 Hopkinton, MA 01748 Tel: 508-435-5040 Fax: 508-435-1530 www.tanejagroup.com