EVault®
A Seagate Company

The best case for the worst case.™

White Paper

Seven Questions to Ask When Considering an All-in-One Data Protection Solution

DISK-O-TAPE, INC.

A Compelling Case for All-in-One Data Protection

Most administrators who consider an all-in-one data protection (DP) solution are looking for the fastest, most cost-effective path to securing enterprise data, as well as the simplest system to manage and support. That's because piecing together a comprehensive solution from separate components is a complex, laborious process that requires research, testing, integration, deployment, perhaps working with multiple vendors, and more. Worst of all, you may have to go through this intricate process just when you need the data protection the most. But while speed and simplicity are important drivers, they won't do you much good if the all-in-one solution you end up with isn't built on best practices. Making sure that's what you get is the focus of this white paper.

All-in-one DP solutions include all of the hardware and software necessary to get up and running quickly:

- **Hardware:** The hardware configuration can vary depending on the type of target customer. Solutions for small and mid-size businesses (SMBs) are often a network attached storage (NAS) server with two or three terabytes of internal storage. Solutions for larger companies are typically server node(s) with SATA or Fibre Channel storage.
- **Software:** All-in-one DP solutions usually come with backup and recovery software. The software may include agents to protect each client, plug-ins for granular protection of applications, management and reporting tools, and a server component that handles the back-end processing. Some solutions also include data deduplication, compression, encryption, bare-metal recovery, and continuous data protection (CDP) functionality. Depending on the particular solution and vendor, these may cost extra.
- **Support and Warranty:** All-in-one DP solutions will typically include support for the backup application and warranty coverage for the hardware. Additional service offerings are almost always available. These can include 4-hour onsite response for hardware repair, training and certification programs, disaster recovery planning and testing, and software implementation.

There are eight things to consider before you make your decision on which solution to purchase. When evaluating solutions, consider the following:

1. What software is included?
As mentioned above, it's important for you to take a look at what software is included in each offering. Some only offer Windows client agents; others charge you extra for data deduplication and/or encryption functionality. It's important to choose a solution that can be adapted to your environment. The best solutions offer broad platform and application support, including protection for Windows, UNIX, Linux and VMWare and key applications. If unlimited agent and plug-in licensing is included, you'll get simple, streamlined management and won't need to purchase backup licenses when you deploy new servers into the environment. Some solutions even let you chose from a menu of client software options for specific platform and application protection.

Make sure it also includes some sort of data deduplication. Data deduplication is the process of identifying and removing or omitting any duplicate data found in an organization's backup data sets. There are various techniques for deduplicating data; most of them will help you improve backup times and use your back-end storage more efficiently. If deduplication is already included in your backup solution, you won't have to spend money on a standalone deduplication solution. This will also minimize complexity and make things a little easier to manage.

Finally, if you have an aggressive Recovery Time Objective for key Windows-based servers, look into a solution that integrates bare-metal restore functionality. By using a single appliance to protect your systems as well as your data, you can shorten your backup window and reduce storage consumption.

2. Who's going to manage the onsite hardware?
Depending on the number of IT resources you have within your organization, you may want to either manage the onsite hardware yourself or outsource the job to experts. If you choose to manage it in-house, make sure that the backup application has an easy-to-use, centralized management console. That way, you can standardize data protection processes universally—even across multiple, geographically dispersed locations.

If you lack the IT resources to manage the solution yourself, consider other options. Some solutions are almost completely "hands off" and require minimal day-to-day interaction. Some solutions are remotely managed by the vendor, allowing you to concentrate on your business instead of your backup vaults.

3. Can the solution support geographically distributed operations?
Some solutions require hardware at each and every location because they are not optimized for data transfer over a wide area network (WAN) or other low bandwidth connections. These solutions use up a lot of network resources and take a long time to complete backup jobs, so they're not ideal for companies with distributed operations. Companies with branch offices should only consider solutions with client-side de-duplication. Client-side deduplication, also referred to as delta processing, compares the latest backup data against the previous backup job's data. Since much of the data remains the same from backup to backup, the application will only transmit the new and changed blocks (deltas) found since the last backup. This feature is invaluable for companies backing up over the WAN since it can shorten backup windows and minimize the impact on their network. (Some solutions also perform back-end deduplication to further reduce the amount of data stored. These can significantly reduce the storage footprint.)

4. Can the solution accommodate data growth?
Over the next 18-24 months your organization will undoubtedly see significant data growth. With all the email traffic, transactions and user files, this is inevitable. Consider a backup and recovery solution that gives you room for future growth. Understand what

it takes to upgrade the solution's storage capacity. This reliance on hardware can cost a lot and adversely impact scalability and performance. Some appliances have a fixed amount of storage; if the amount of backup data outgrows the appliance, then you have the hassle of retiring the old appliance and replacing it with a new one. Other solutions scale in one- or two-terabyte nodes. Each node, though, can cost in excess of $30,000 dollars. This can get terribly expensive, very quickly.

More flexible appliances support storage expansion within the same chassis. Unused bays can hold additional disk drives, but they need to be configured to meet your redundancy standards. Work with your vendor to plan an expansion that meets your RAID requirements.

Appliances with inactive RAID storage that can be activated with a software license give you, by far, the easiest path to storage expansion.

It's wise to consider a solution that allows you to share the storage with applications other than your backup.

5. Can it easily store redundant copies of your backups in the cloud—even if the appliance itself fails?

For most companies today, onsite backup is not enough; they need a redundant copy of their backup data to mitigate the risk of a complete site outage. When considering an all-in-one solution, make sure that it gives you the flexibility to replicate to another disk-based vault located at either a designated disaster recovery (DR) site or the cloud. As costs for disk storage continue to drop and virtualization becomes more popular, "D2D2D" (disk-to-disk-to-disk) and "D2D2C" (disk-to-disk-to-cloud) options are becoming increasingly attractive over relatively inefficient and error-prone tape recovery services. And since you have two copies of your backup data—one stored onsite and one stored offsite in the cloud—you can benefit from LAN-speed recoveries; and, in the event of a complete site outage, you can continue to back up to and restore from the offsite location.

If you have an aggressive RTO, you may also want to consider replicating to a cloud storage service provider that offers a remote disaster recovery service. These services offer a "warm site" that is continually standing by, giving you the ability to quickly recover key systems and data if a disaster were to strike. You can get your operations back up and running within a virtual environment within 24 to 48 hours. Some services also offer a team of experts that can guide you through the entire recovery process.

6. How is the data secured?

Encryption is critical for successfully protecting backup data. Most solutions offer encryption, but pay close attention to when and how the backup data is encrypted, as well as the impact on backup and restore times. Only consider solutions that support AES-level encryption. Some solutions offer end-to-end security, allowing you to encrypt your backup data at the source (client), while in transit, and at rest on the disk target. If the backup data is being replicated to an alternate or hosted site, you may also want to look into solutions that allow you to restrict access to any encryption keys associated with the stored data.

Also consider the potential impact on speed of backups and restores. While some performance hit may be necessary if encryption is deployed, some vendor solutions may differ in terms of the degree of impact. Learn what the vendor has done to reduce the performance impact of the encryption process.

7. What is its power consumption profile?

Many data centers today are approaching ceilings on available power, cooling, and floor space, so IT administrators are looking into more efficient IT solutions including all-in-one solutions for backup and recovery. Green solutions that are energy efficient in terms of direct power consumption, and cooling requirements are now available.

Consider solutions that leverage MAID (Massive Array of Idle Disks) technology. The basic premise of MAID is to step down power consumption on the hard drives when they are not in use—similar to a laptop or desktop PC. A good example of this is Nexsan's SATA storage arrays. Nexsan storage systems use multiple power saving modes to balance energy consumption with performance and availability. After a period of inactivity, they can automatically slow the hard drives down to save power. When needed, the hard drives can rapidly return to active I/O duty without incurring a time delay or power spike.

A Case in Point—Medical Business Service

Medical Business Service, a nationwide patient billing services company head-quartered in Coral Gables, Florida, recently purchased an all-in-one EVault® data protection solution from EVault. CIO Syed Faisal chose an all-in-one solution because of the versatility of the EVault backup application and the price.

"In the end, the price was right and the technology was there to support our infra-structure," he said, noting, "We liked the fact that EVault started bundling a server and storage with EVault Software to create a pre-configured all-in-one appliance. I also liked the fact that EVault was part of Seagate, who is a leader in hard disks and storage."

Faisal has since implemented two EVault Plug-n-Protect appliances, one at the primary data center, and the second ready at the company's Georgia office. Backup data will be replicated between the two appliances, to ensure fast recovery from either location. After what he reports was a "surprisingly quick" implementation process, he couldn't be happier with the results he's seen so far.

Conclusion

There are a lot of all-in-one data protection solutions on the market today. They're becoming increasingly popular because they are so easy and economical to procure, deploy, and maintain. But make sure to take a look under the hood as not all solutions are the same. It's best to go with a vendor that offers flexibility and includes a range of services. You want to be able to grow with the solution as your needs change and environment becomes more complex.

Take the Next Step

To learn more about EVault backup and recovery services, contact Disk-O-Tape, Inc. by phone at 800-923-8273 or 216-765-8273, or email at evault@disk-o-tape.com, or visit www.disk-o-tape.com

23775 Mercantile Rd. | Cleveland, OH 44122 | **T.** 800-932-8273 | **F.** 216-765-0436 | **E.** evault@disk-o-tape.com | **www.disk-o-tape.com**

EVault® A Seagate Company

Headquarters | 201 3rd Street | Suite 400 | San Francisco, CA 94103 | 877.901.DATA (3282) | **www.evault.com**
NL (EMEA HQ) +31 (0) 73 648 1400 | **FR & S. Europe** +33 (0) 1 55 27 35 24 | **DE** +49 89 1430 5410 | **UK** +44 (0) 1932 445 370
Brazil 0800 031 3352 | **Latin America** Evault_latin_america@evault.com

2013.05.0016_wp_ss-cb (updated 05/09/2013)