White Paper

i365
A Seagate Company

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

A Compelling Case for All-in-One Data Protection

Many administrators who oversee their organization's backup and recovery are considering an all-in-one data protection (DP) solution because it can greatly simplify the procurement process, expedite deployment, and get their critical systems and data protected that much sooner. These solutions also tend to be less expensive than buying each component separately. What's more, they give administrators a single point of contact for all their support needs. This trend is supported by a recent survey conducted by the Enterprise Strategies Group (ESG). In that survey, more than half of the respondents—both small and mid-size businesses—indicated that they "would prefer to rely on a single vendor for their data protection solutions whenever possible."[1]

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.

RECOVERY POINT OBJECTIVES (RPO)

In addition to setting Recovery Time Objectives (RTO) when establishing a disaster recovery plan, organizations will also set Recovery Point Objectives (RPO). This is done by setting a limit to the acceptable amount of data that can be lost after an interruption or site outage. In general, the more frequent your data is backed up, the more aggressive your RPO can be. Your RPOs can also determine the appropriate recovery solutions and services.

CONTINUOUS DATA PROTECTION

Continuous Data Protection (CDP) technologies minimize potential data loss by continuously tracking changes and generating recovery points. CDP solutions range in price and degree of protection. For most applications, near-CDP solutions that generate recovery points as frequently as every five minutes are sufficient.

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. 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 includes bare-metal restore functionality.

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 my estimated rate of 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. Some solutions may require a significant investment in specific branded hardware in order to run deduplication and other space-saving technologies. 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.

Some solutions are designed to run efficiently and scale without a lot of specialized hardware. These solutions can often rely on software-based optimization technologies to help reduce the amount of backup data processed, transmitted, and ultimately stored on disk. They usually consist of a server head and storage array. The storage can be SATA or SAS and can hold anywhere from 14 to 42 one-terabyte drives, giving you plenty of room for growth.

It's wise to consider a solution that can be configured as a Storage Area Network (SAN). This allows you to share the storage with applications other than your backup.

5. Can the solution give you affordable offsite protection for disaster recovery?

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 team of experts that can guide you through the entire recovery process.

6. What security features does the solution offer?

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. How green is the storage?

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.

8. Can the solution meet my Recovery Point Objectives (RPO)?

Your ability to achieve a target RPO depends on how frequently you back up your data. If you back up your data once daily at midnight, your RPO is 24 hours. In the event of a system failure, any new or changed data after that point will be lost, so your data exposure is 23 hours and 59 minutes. While this may be acceptable for data kept on a home computer, most businesses require smaller window of exposure, perhaps down to five minutes. Take this into consideration when shopping around for an all-in-one backup solution. Some all-in-one solutions include continuous data protection (CDP) or near-CDP capabilities. CDP technologies minimize potential data loss by continuously tracking changes and generating recovery points as frequently as every five minutes. This approach represents a tiered recovery architecture—a methodology of applying the right backup strategy and solution that's appropriate for the data you are backing up. The most mission-critical data, for example, should have backups that include disaster recovery, bare metal restores and CDP. Less valuable data can be backed up with less-aggressive frequency and with longer RTOs, reducing costs.

A Case in Point—Medical Business Service

Medical Business Service, a nationwide patient billing services company headquartered in Coral Gables, Florida, recently purchased an all-in-one EVault® data protection solution from i365. 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 infrastructure," he said, noting, "We liked the fact that i365 started bundling a server and storage with EVault Software to create a pre-configured all-in-one appliance. I also liked the fact that i365 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 storage solutions, call us at 1.877.901.DATA (3282), email us at concierge@i365.com, or visit us at www.i365.com.

[1] Data Protection Market Trends, The Enterprise Strategy Group, Inc., by John McKnight and Mary Johnston Turner with Heidi Biggar, Jennifer Gahm and Lauren Whitehouse, January 2008

i365
A Seagate Company

Headquarters | 3101 Jay Street, Suite 110 | Santa Clara, CA 95054 | 877.901.DATA (3282) | **www.i365.com**
Netherlands (EMEA HQ) +31 (0) 73 648 1400 | **France** +33 (0) 1 55 27 35 24 | **Germany** +49 (0) 89 28890 434 | **UK** +44 (0) 1932 445 370