Backup Software Buyer's Guide – part 2

Your expert guide to backup software

In this e-guide

Five challenges when buying backup and restore software

George Crump, President

Backup software is a mature product category, so it can be tough to select a vendor. Discover the most important factors when choosing the best product for your environment.

Editor's Note: *This is part three of a four-part series on backup software applications. Part one explored what backup software does. Part two discussed the relevancy of backup software applications in today's IT world. Stay tuned for part four, which will provide information on how to select the right backup software for your organization.*

Trying to cross-correlate how one vendor implements a product feature and compares it to another is a daunting task. Backup software moves data through almost the entire data center infrastructure, so implementing it, training staff and obtaining support for it is no small feat. The request for proposal for backup and restore software has to take into account all these factors to ensure the organization has a viable long-term data protection strategy.

Here are five challenges organizations will encounter when buying backup software.

In this e-guide

Challenge 1: The support offered by backup software vendors

Support should be the most heavily weighted factor in any backup and restore software vendor selection. Backup software touches almost every corner of the data center, so the chances of it not interoperating -- or working at one point and later breaking -- are high. For these reasons, organizations need to consider a backup software vendor's ability to provide quality support and training.

Surprisingly, some of the best technical support is available from sources other than data backup software vendors. Resellers, for example, often provide excellent backup infrastructure support. The reason for this is that the backup software is often *not* the component that is broken; the problem is how that software interacts with the server hardware, storage adapters, operating systems (OSes) and applications. A reseller often has better training on the environment as a whole, while a backup software vendor may only know its particular software. Backup software vendors can point at the component in the environment that is causing the problem but, unlike a reseller, they often can't do anything to fix or work around that problem.

In this e-guide

Challenge 2: It is a game of chess, not checkers

One of the most important requirements of any backup and restore software is that it support the various OSes, environments (VMware) and applications (Oracle, MS SQL and Exchange) in your environment.

Seeing which system the backup software can support is easy. The chess part of the equation is to ensure vendor support of the needed platform is more than just a checkbox. Typically, an organization will want the protection of these platforms to exploit various capabilities.

The specific feature you should look for largely depends on whether an organization is trying to implement a single backup process or filling some holes the current backup software doesn't cover.

Many organizations are more than 50% virtualized, so virtualization-specific capabilities are important. Backup software should also have the ability to back up off-host virtual machines, which means there is no need to install the backup agent within the VM or physical host. All modern backup applications should leverage change block tracking, which sends only the changed segments within a backup to be transferred to the backup device.

Recovery is another area that has seen significant improvements in virtualized data protection. Look for software with in-place or instant recovery features. If there is a physical server failure or data corruption, instant recovery allows a VM to access a protected copy of its data store directly from backup storage. This saves the time it would have taken to transfer data over the network.

Business-critical applications -- like Microsoft Exchange, Oracle and SQL -- provide application programming interface access to the database to protect it while online. Look for an application that supports these APIs. Applications should also restore data at a more granular level -- mailboxes, individual messages or tables -- than just the database itself.

Challenge 3: Protection from a 30-day evaluation

Backup and restore software is typically available as a 30- or 45-day evaluation. The expectation is that IT professionals can test all the features and capabilities of the software, as well as perform stress tests to see how it holds up under extreme circumstances in that evaluation window. Pushing the software to the limit is important. The goal is to simulate the use of the software over the course of several years. While testing basic backup and recovery is relatively straightforward, the reality is that IT professionals will rarely be able to simulate the long-term use case within 30 days.

Specific weak points require testing; most importantly, the metadata the software creates. This metadata points to the location of all the data and the data versions the software protects. Rapid searching and updating of the metadata is important to long-term use, and many backup applications lag in this area. Simulation of metadata weak points can include writing the same data over and over again to the system and then searching for a specific version of that data.

The reality is that no one can test everything. A request for proposal (RFP) should include some form of protection from unforeseen problems in the software that allows a company to receive free technical support or even a partial refund in the event of a problem. The wording has to be precise because, if done incorrectly, publicly traded companies may not be able to recognize the revenue spent on the software due to a penalty associated with nonperformance.

Challenge 4: Thinning the herd

Backup software is often surprisingly expensive, but it is an extremely competitive business because of the number of vendors in the market. Companies should look at the RFP as a way to thin the herd, but should certainly go back to companies for a "best and final" after the creation of the short list of vendor finalists. In almost every case, when buying backup software, the goal is to replace a product that is already in place. Organizations

should specifically request a competitive trade-in as part of the RFP and look for ways to leverage this purchase as a means to get additional discounts on other products the vendor may sell.

Challenge 5: Price isn't everything

The software a business buys will protect one of the organization's most valuable assets: data. Losing this asset, even temporarily, can be costly. Organizations should therefore talk to prospective vendors about any additional value the software can provide. For instance, several backup software vendors now provide copy data management capabilities to reduce the need to create redundant copies of data throughout the enterprise.

Organizations and vendors need to establish a partnership instead of a customer vs. supplier relationship. Backup and restore software tends to be implemented for the long term, so liking your vendor will make that time much more comfortable.

Next article

In this e-guide

Which enterprise data backup software is right for your business?

George Crump, President

Explore whether backup software for the whole enterprise or environment-specific data protection is the better bet for your organization. The cloud can be an option, as well.

Editor's Note: *This is part four of a four-part series on backup software applications. Part one explored what backup software does. Part two discussed the relevancy of backup software applications in today's IT world. Part three discussed the five challenges when buying data backup software.*

Backup software is "sticky." Once IT picks the backup software it wants, it tends to stay in use for years -- if not decades. The reason for the adhesion is not because the IT team is in love with the software. Often, the implementation process was so bad that the team fears going through it again with another product.

Having backup software that fits your organization is vital. Even though implementation causes headaches and instills fear in even the bravest of IT professionals, it's important to reassess your backup application and seek a new one if it's warranted. There is backup software that will apply to your entire enterprise. But while some backup offerings can hit general checkboxes, others

concentrate on specific applications and can solve problems that an overarching backup product cannot.

When the time comes to make the switch or install your first enterprise data backup software application, it is critical to articulate the organization's goals for data protection. Make sure the potential backup software -- whether all-encompassing or niche -- and vendor will meet those goals. In general, most organizations will need multiple data protection products to meet all of their data protection goals.

Evaluating enterprise backup software suites

If your goal is data protection, you should consider an overarching backup application that handles bare-metal database applications, virtual environments, laptops and desktops and that integrates with the cloud. These options are limited.

Enterprise data backup software attempts to provide support for your entire data center by giving you one product to manage and one vendor to handle. The challenge with these apps is keeping pace with the rate of change. For example, the majority of enterprise data backup software vendors took so long to fully support virtualized infrastructures that newcomer Veeam Software

seemingly came out of thin air to become a major player in the backup business.

The good news is that enterprise applications usually have rock-solid support. A good example of this support is how well these applications support bare-metal database server environments like Oracle and Microsoft SQL. However, their size can slow them down if they lack support for the modern NoSQL applications establishing a foothold in enterprise IT.

Enterprise backup applications include Commvault, EMC NetWorker, HPE Data Protector, IBM Spectrum Protect, Unitrends Enterprise Backup and Veritas NetBackup. These applications all have strong bare-metal application support and, in most cases, are making gains with virtualization and laptop or desktop backup. Still, their support in these formerly niche areas may not be as robust as applications that specialize in those types of data protection.

You will have to do some testing to determine if these features meet your needs. If those test results are good, you can consolidate to a single enterprise backup software suite. If not, you may need to add more environment-specific data protection applications.

Enterprise backup software applications are a good choice for those looking for a wholesale replacement or who have general backup requirements. More often than not, specific functions require more focus. There are some niche backup

software vendors that address environment-specific data protection issues like NoSQL and the cloud.

Environment-specific data protection

Running multiple applications for data protection is nothing new. Environment-specific data protection was around long before enterprise backup even existed. Many IT organizations will use environment-specific products until slower-moving enterprise backup applications catch up in quality. For example, in the 1990s, there were dozens of database-specific applications providing online backup support for applications such as Oracle and Microsoft SQL. But most of those were replaced as enterprise applications enhanced their backup support.

There is much the same situation occurring in the data center today with virtualization. It is common for a virtualized environment to be protected by an application from Nakivo, Unitrends or Veeam. If an organization's data center is 100% virtualized, or at least close to it, then the virtualized application is essentially an enterprise app, and the organization may consolidate around this "point" offering.

Virtualization-specific applications are usually easier to implement than their enterprise alternatives and tend to more fully exploit virtualization data protection features. Many of these apps are now adding enterprise features like

tape support, bare-metal backup support and cloud support, blurring the line between environment-specific and enterprise products.

Does NoSQL equal no backup?

A gaping hole in most enterprise data protection offerings is the lack of support for modern applications like Cassandra, Couchbase and MongoDB that are built on NoSQL. Similar to the situations with online database backup and virtualization backup, enterprise data backup software is slowly moving toward supporting them, but, in some cases, they may be years away from full support. In the meantime, NoSQL data protection looks very similar to the early days of database protection with administrators cobbling together scripts or using environment-specific applications, like Datos IO.

The cloud, the cloud, the cloud

IT can use the cloud in a variety of ways for data protection. For example, it can be an extension to existing data protection applications where IT stores old backups in the cloud instead of on site. In this scenario, the enterprise has to be careful to calculate the long-term, repetitive cost of the cloud versus the upfront cost of owning its own storage.

In this e-guide

An alternative consideration is a cloud-only (or mostly cloud) deployment option from vendors like Asigra, Axcient, Datto, Infrascale, Zetta and others. These vendors deploy their backup software as a service. This results in low or no upfront cost.

Vendors also tend to use an agentless approach, meaning there is no software to deploy on the organization's servers. These applications typically provide an on-site appliance that receives the backup and replicates it to the cloud. As a result, the data center has the most active data on site for rapid recovery and all of the data off site in the event of a disaster. Many of these services also offer disaster recovery as a service to enable them to not only store data in the event of a failure, but to host the data center's applications for a period of time.

Cloud-based backup technology must go through the same qualification process that enterprise data backup software does. IT must verify that the product will cover the organization's most critical applications and environments. Then, the administrator must address specific cloud questions, like how quickly will the organization get its data back if there is a failure? Or, if the service offers DRaaS, the organization needs to understand how quickly its applications can be ready in the provider's cloud and return service to its own data center.

In this e-guide

What's the best backup software for you?

There is no one backup software application that is perfect for all data centers. Each IT organization needs to test and evaluate these products for themselves. Enterprise backup still offers the best chance at consolidation, but the organization may have to accept some compromise on features.

Virtualization-specific applications may also provide a point of consolidation, especially as virtualization products begin to offer physical system backup. The cloud doesn't change the software consideration, but it does offer a new purchasing model and a new destination. Organizations looking to outsource backup, recovery and disaster recovery may find the cloud very appealing.

About the author

George Crump is president of Storage Switzerland, an IT analyst firm focused on the storage and virtualization segments. With 25 years of experience designing storage solutions for data centers across the United States, he has seen the birth of such technologies as RAID, NAS and SAN. Prior to founding Storage Switzerland, George was chief technology officer at one of the nation's largest storage integrators, where he was in charge of technology testing, integration and product selection.