10 Purchase Considerations for Enterprise-Class Endpoint Backup and Data Availability Solutions
The need for endpoint backup is nothing new for IT administrators. It remains vitally important to keeping employees productive and the business running in the face of accidents and disasters that cause employees to lose valuable data. Like everything else in IT, the endpoint backup and recovery process continues to evolve, perhaps never more so than in the last five years. The proliferation of mobile devices and the adoption of cloud computing environments mean that the enterprise has been extended beyond the confines of the office. The sheer number of endpoints that exist today means the devices — such as laptops, smartphones and tablets — are that much harder to manage, secure and back up.

Today’s businesses are creating data at an astonishing rate, and the devices end users are using to access and store this data can hold more data than ever before. This not only makes the process of backing up the data more important, but it makes it more difficult. The data needs to be transported, secured and made available to the people who can access it when they need it. Given today’s distributed environments with multiple devices and the steep cost for data breaches and downtime, that’s a lot to ask of an endpoint backup solution.

As we’ll see in our list of 10 purchase considerations, IT administrators have a lot to think about when they are exploring enterprise-class backup and protection solutions, but vendors in this space are putting a lot of thought into products that provide the backup businesses need, but also go beyond backup to help with other issues IT departments face related to today’s explosive data growth and the multitude of devices available to users.

Backup and data protection solutions can only do their job when they’re used properly. That’s why we’ll begin our list of purchase considerations with the end user.
1. End-User Experience

End users need to use their endpoint devices to keep in touch with clients, produce documents and interact with corporate applications like CRM and email on a regular basis. Backup is a top-of-mind issue for IT managers but it’s not something end users think about very often, unless of course they need to restore data that’s lost.

**Non-Intrusive:** Endpoint backup solutions should be nearly invisible to end users, lest they interfere with their daily work and the user finds a way to stop the application or circumvent it. Antivirus vendors have had to toe this line for many years — some better than others — and know firsthand how useless apps can be when they’re not used. Slow machines and stalled applications caused by backup and security apps could lead to an increase in help desk and support tickets, which consume IT resources better used elsewhere in the organization.

**WAN-Optimized:** Since today’s employees take maximum advantage of the mobility available with laptops and mobile devices, IT administrators can’t rely on only the office network to help transport data during backups. This means enterprise endpoint backup solutions need to use whatever network is available to them at the moment: in the office, at home, at the airport, the coffee shop or on a plane. The availability of bandwidth and quality of the connection can vary greatly among these locations, so a solution with WAN optimization, bandwidth throttling and auto-resume capabilities can go long way toward ensuring backups are successfully completed regardless of the networks used.

**End-User Control:** Finally, some businesses may want to give some end users control over certain elements of the endpoint backup process, such as frequency of backups, file inclusions/exclusions, etc. A solution that allows administrators to grant granular control is usually a good idea. Many businesses will not issue control to end-users, but others will allow a small group of Power Users, perhaps on the IT staff, to have more control over the process.
2. Global Data Deduplication

We’re creating more data than ever before, and that poses new problems that older approaches to backup didn’t need to consider. Backups now require more time, more bandwidth and more storage, all of which cost more money and increase the risk that backups will not go as planned.

Fortunately, not all of the data we’re creating is original. When an email goes out to seven people in the organization, for example, it gets downloaded to seven different endpoints. By some estimates, more than 80 percent of enterprise data is duplicated elsewhere in the enterprise. Backing up the same message seven times is not the best use of time, bandwidth or storage. That’s why many vendors working in the backup space, and increasingly in other areas of data storage as well, are turning to deduplication technology to reduce the amount of data that gets stored, which means that data takes up less storage space and consumes less bandwidth because all seven email messages aren’t making the trip on the network.

Global: Not all data deduplication is built alike; and while dedupe of some kind is now considered essential to backup and restore, there are a few deduplication features that can make a big difference when it comes to the deduplication of endpoint data. Global deduplication not only backs up a single block of data across all of the files on a device, it also only backs up a single block of data across all of the devices. If 80 percent of the data in the enterprise is duplicate, then global deduplication offers significant savings when transporting and storing data.

Client-Side: Deduplication can be done on the client side or on the server side. For the purposes of enterprise endpoint backup, client-side deduplication is the preferred method because it cuts down on the number of round trips the data needs to take, thereby conserving bandwidth.

Scalable: Finally, there are methods of deduplication that offer client-side caching of data and innovative caching and support for solid-state disk (SSDs) on the server-side, all of which can help speed up and scale up the deduplication process to handle large amounts of data.

<table>
<thead>
<tr>
<th>How would you deploy an endpoint protection solution?</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th></th>
<th>2010</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-premise</td>
<td>60%</td>
<td>40%</td>
</tr>
<tr>
<td>Cloud</td>
<td>20%</td>
<td>30%</td>
</tr>
<tr>
<td>Mixed</td>
<td>10%</td>
<td>10%</td>
</tr>
<tr>
<td>Hybrid</td>
<td>0%</td>
<td>5%</td>
</tr>
</tbody>
</table>

Source: Druva customer survey 2010 and 2012. Results from 400+ responses.
3. Flexible Deployment Options

One of the benefits of cloud computing is that it allows businesses that may not have the resources to deploy, maintain and support an enterprise application to take advantage of enterprise-level software and functionality. While deploying an application in the cloud might hold more appeal for smaller businesses than larger enterprises, finding an endpoint backup solution with flexible deployment options gives businesses of all sizes some flexibility if their situation changes.

The decision to deploy in the cloud or on-premise usually takes into account budgets, time, IT staffing, internal company policies or external compliance regulations, investment in IT infrastructure and the comfort level with software-as-a-service (SaaS).

Source: Druva customer survey 2010 and 2012. Results from over 400+ responses.

On-Premise: If a business chooses to deploy an on-premise endpoint backup solution, it will want to examine how many users can be supported on a single server and available deployment and management options for users, groups and endpoints.

Cloud: When choosing a cloud-based deployment of endpoint backup, businesses will want to learn what they can about the cloud provider, security and the service level agreement (SLA) that governs application availability.

Hybrid: Businesses should also be able to deploy a hybrid model that combines the benefits of on-premise and cloud deployments, e.g., an on-premise deployment leveraging the cloud for disaster recovery, a cloud deployment replicating to an on-premise server for better speed, etc.

4. Easy Deployment & Configuration

IT administrators want backups to be as easy as possible: Download (or install), configure, deploy it and manage the backup application. Backup software that’s small enough to easily download is a good start.

Quick Configuration: Configuration is easy to accomplish when the solution comes with pre-configured user profiles, which will cover the vast majority of the user types in an organization, as well as the ability to easily create custom user profiles.

Backup and recovery solutions are going to be using the same data stores on an endpoint repeatedly, so some method of easy configuration that makes it easy to target common data sources like email and document stores will also make configuration easier.

Mass Deployment: Enterprise application deployment is always a potential headache for administrators, so any endpoint backup solution should feature a mass client deployment option that takes advantage of existing investments in technologies like Microsoft Active Directory, Microsoft System Center.
Configuration Manager or similar products.

**Auto Upgrades:** Finally, an enterprise endpoint backup solution that deploys automatic client upgrades without involving a lot of manual interaction on the part of administrators, and without involving end users, is the most efficient way to handle updates.

**5. Enterprise-Grade Scalability**

One of the easiest ways to protect a software investment is to ensure that applications purchased for the business today will also work for the business tomorrow and the day after.

**Large Number of Users and Data:** When it comes to endpoint backup applications, this means the ability to scale as the number of employees increases, the number of devices grows and the amount of data increases.

**Unified Management:** As any and all of these numbers increase, administrators will want unified management so they can manage the backup solution across servers, storage environments and physical office locations. Administrators will also want to take advantage of the mass deployment options we discussed earlier and integration with tools like Microsoft Active Directory.

**On-Demand:** To help ease the storage burden, cloud-based storage on demand is a feature increasingly being offered by vendors whose applications have a need to scale quickly to handle new users or an increase in data. Being able to tap the unlimited storage of the cloud without having to find and configure a cloud service on your own means that users don’t need to worry about capacity issues.

**6. Enterprise-Class Security**

Much of the data that lives on enterprise endpoints is sensitive in nature. It may not all be subject to industry or government security standards, but internal documents are internal for a reason. Businesses need to make copies of this information so it’s available to them in case of a system failure, device loss or accidental deletion, but those copies need to be secured throughout the entire backup process.

**Data Encryption:** Data is usually most vulnerable when it’s in transit. Endpoint backup solutions should
feature 256-bit SSL encryption for data in transit and 256-bit AES encryption for data in storage.

Certifications: For backup solutions that utilize cloud-based resources, look for certified cloud infrastructures such as SAS-70 and ISAE 3000. Additionally, PCI DSS Level 1 and ISO 27001 certifications are good, too.

Encryption Key Management: Some cloud providers use the same encryption key for all of their users and fail to compartmentalize data from their multiple customers. Look for cloud providers that use unique encryption key management for each customer and unique authentication and access control for each customer.

To ensure no one has access to the backed up data, some vendors offer two-factor encryption, which uses a unique distributed encryption key management system that allows no one, including the company storing the data, to gain access to a customer’s encrypted data except the customer with access credentials.


7. Integrated Data Loss Prevention

With the proliferation of laptops and mobile devices, the concepts of backup and mobile device management are starting to blend. It’s important for an endpoint solution to prevent data loss from lost or stolen devices, so critical corporate data does not end up in the wrong hands.

Endpoint Data Encryption: Integrated data loss prevention features include device encryption that encrypts critical data on the endpoint device. Encryption ensures that stolen devices don’t expose data in clear text. It’s important for the right encryption solution to not interfere with end users’
productivity as they access device data continuously.

**Remote Deactivation:** Remote wipe capability, which allows an administrator to wipe data off of a mobile device in case of loss or theft, is also gaining in popularity as devices get smaller and much easier to misplace. To cover all cases, it’s important that the remote decommissioning can be initiated both manually by the administrator and automatically from the agent on the device.

**Geo-Location:** Finally, device geo-location features help locate lost devices and aid in their recovery by using the device’s coordinates. It’s important that the device be tracked within 10-20m accuracy.

By combining mobile device management with endpoint backup, there’s one less vendor businesses need to deal with and the door is open for further integration between backup and device management.

8. **Mobile Access & Data Protection**

Mobile devices such as smartphones and tablets have an additional need for IT policy management for businesses that have or are considering a bring-your-own-device (BYOD) policy.

**Mobile Access:** It’s important that users get access to all their backup data from their own mobile devices such as iPhones, iPads and Android devices. IT needs to be able to enable or disable mobile access as a BYOD policy.

**Mobile Backup:** The variety of mobile devices also means that vendors selling endpoint data protection solutions have to support backup for iOS and Android devices. More than just access devices, these devices increasingly help in content creation. It’s important to have policies for the optional or mandatory backup of critical corporate data from these mobile devices.

**Mobile DLP:** Data loss prevention for mobile devices is equally important given how much critical corporate data
now resides on these devices. Look for data loss prevention features like those mentioned above that apply natively to mobile devices, such as remote device deactivation, encryption and geo-location. Look for solutions that can protect both iOS and Android devices.

9. Integrated File Sharing & Collaboration

This is another area that goes beyond backup but is likely to increasingly get attention from backup and recovery vendors. The ability to easily share and collaborate on files is becoming an increasing thorn in the sides of end users and IT administrators as the need for file sharing grows and administrators limit the solutions that can be used within the enterprise. This is causing end users to turn to consumer-grade services for sharing files, sometimes in violation of company policy.

*Easy File & Link Sharing:* Functionality that enables both peer-to-peer file sharing and ability to collaborate with external users on files through links to the file instead of relying on email is more secure and easy to use for end users. Real-time sync of files and folders across multiple user machines ensures all involved are using the same copy of the file.

*Device Sync:* Given that today’s users own multiple devices, real-time sync of selected files and folders across multiple devices ensures easy access to all data from any device.

*Security & IT Visibility:* IT needs to get increased visibility into sharing activities and be able to set policies to ensure the security of critical corporate data. Rich reporting and activity streams combined with deep IT policy management offers IT a solution that they can bless within the organization.

*Common Infrastructure:* Backup providers sense an opportunity in the file sharing space. These vendors already have the infrastructure to help store, transfer and deliver them when needed. They can also use their expertise in data deduplication and user management to make the process smoother and more controlled.

*Unified Management:* When governed by centralized policy management, integrated file sharing and collaboration can present large savings in time and effort for administrators.

10. Data Analytics and Compliance

Endpoint backup and recovery solutions can provide a valuable window into the business, as well as help IT administrators for the future by enabling them to analyze the types of data users are creating and storing.

*Reporting & Alerts:* Enterprise endpoint backup applications should include reporting that allows administrators to monitor the application and its usage and get an understanding of the storage and bandwidth requirements they will need to keep reliably backing up data in the future. By the same token,
the system should include alerts and notifications that inform administrators of important information about the application.

**Data Composition Analysis:**
Information on data composition and trends gained from endpoint backup can also provide valuable information to administrators, such as examining what kinds of content are currently stored on endpoints and how.

**Federated Search:** Finally, the presence of real-time federated search capability that can find files across any endpoint device across the organization can prove valuable to administrators, so they can track confidential data on endpoints and act on them.

**How Druva Can Help**

As we’ve seen, IT administrators have a lot to consider when shopping for an enterprise endpoint protection solution. Finding a solution that appeals to end users and IT administrators is a challenge, but it’s not impossible.

Druva inSync uniquely offers a full suite of endpoint protection including award-winning backup, file sharing & collaboration, and data loss prevention across all endpoints including laptops, smart phones and tablets. By integrating these solutions Druva helps IT manage the end user data cost effectively and efficiently.

InSync is built with both IT and end-user experiences in mind. IT gets the peace of mind that corporate data on endpoints is safe, secure and compliant. End users get the ability to access their data from any device any time and share files with coworkers.

Druva inSync offers both cloud or on-premise deployment options with enterprise-grade scalability and security, low total cost of ownership and a non-intrusive client that doesn’t hinder end users.

Druva was named Gartner Cool Vendor for Storage and Backup for 2012, and has over 1250+ enterprise customers across 46 countries, which include PwC, McAfee, NASA and Xerox.

To learn more about Druva inSync, visit [www. Druva.com](http://www. Druva.com).