druva

White Paper

5 Critical Considerations for Enterprise Cloud Backup

This guide is written for IT professionals who play a part in data protection and governance at their enterprises. It is meant to provide an initial framework to evaluate cloud backup solutions for endpoint backup.

druva

White Paper

Executive Summary

Your workforce is going mobile, and so is your data. Today, an increasing volume of corporate data resides outside the firewall on end user devices such as laptops, smart phones and tablets. Backing up this data is business critical, yet today's on-premise backup solutions such as tape drives, external hard drives, and network backups are no match for this shift.

For this reason companies are moving to a cloud-based backup solution. Backing up your company to the cloud can be a great proposition, eliminating the need to purchase, install, and maintain internal infrastructure, while allowing you to reap the benefits of the cloud, including 24/7 data access for users, fast transfer speeds, global reach, and on-demand scalability.

Choosing the right cloud backup service is essential to ensure adequate protection, security, and availability of enterprise data. When considering enterprise cloud backup for laptops and mobile devices, keep these 5 critical considerations in mind.

1. Data Security and privacy for your enterprise cloud

Security is job one for any enterprise backup solution, so when evaluating the security of cloud backup solutions, limit your search to one that is certified compliant with international standards such as SOC 1 and ISAE 3000 Type II. These external audits assess all aspects of cloud infrastructure, operations, and control, including facilities, physical security, storage and network infrastructure, firewalls, network configuration, account management, and more.

Encryption is also vital to data protection, but it is not always a guarantee of security and privacy of business data. This particular fact became glaringly apparent after the NSA PRISM program was exposed. If encryption keys are held with your data in the cloud, a provider can be compelled to produce your data under subpoena. Additionally, there are concerns about the potential of a rogue employee at your provider having access to your encryption keys.

Some service providers have responded to these concerns by purporting to "escrow" the key, utilizing a third-party escrow service, saving it separately from data, and rotating it frequently, but a subpoena can still force these service providers to produce customer data. Another response has been to use an onsite server, behind the client's firewall, to house encryption keys in order to guarantee sole ownership, but this introduces hardware to manage and an additional point of potential failure.

For maximum privacy, digital envelope encryption is the recommended solution. With digital envelope encryption, the encryption key is further encrypted using customer admin credentials, and only a token is stored in the cloud

Your corporate data is no one's business but your own, so be sure to pick a cloud provider that will offer rock solid security for peace of mind.

2. 'Always-On' Access and Uptime

Of course, most of "the cloud" actually exists at ground-level, supported by many connected servers and other devices which require electricity and protection from the elements. As much as dependability of data centers has increased over time, these server farms are still vulnerable to power outages, sabotage, and natural disaster.

This is why it's important to carefully understand backup providers' Service Level Agreements. Many providers don't offer automatic data redundancy across multiple data centers, so in the event of a power supply disruption, service is suddenly unavailable and files are out of reach. A natural disaster or catastrophic system failure can even result in permanent data loss.

To account for these possibilities, leading service providers offer data redundancy across multiple facilities, each of which is physically separate, located in lower risk flood plains, and fed via distinct grids from independent utilities. These facilities are connected to different networks to ensure the highest data availability and durability possible.

Be Prepared for the Next Hurricane Sandy

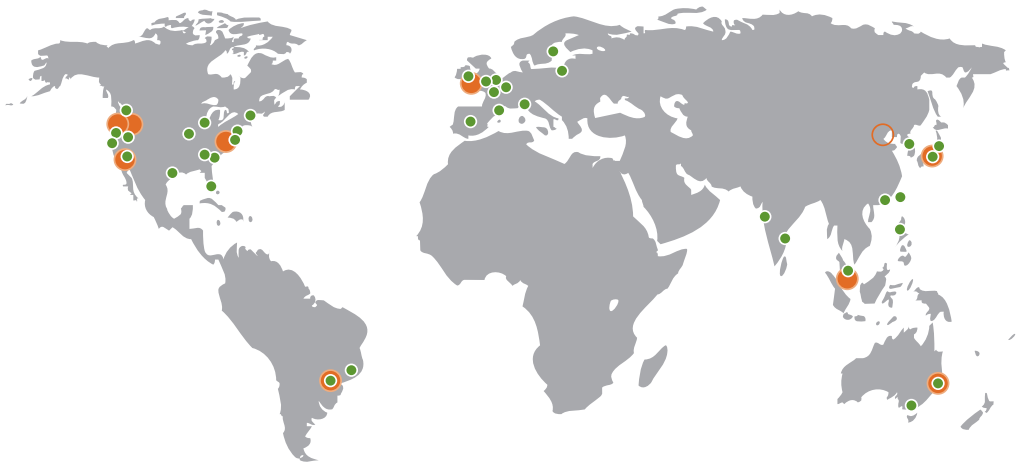
A sudden natural disaster like Hurricane Sandy or the Tohoku earthquake can have serious implications when data centers reside in affected areas. Make sure your cloud backup provider offers geographic backups to other regions, to ensure that data access can continue unaffected in the case of any data center outages.

3. Adherence to data residency requirements

As your business grows, you will need a global backup footprint that complies with regional data protection requirements to enable administrators to map users via profiles to regions, ensuring data resides in the location required.

Traditionally, cloud backup providers have employed a limited number of data centers and housed those data centers within the borders of a single country. As global enterprises support internal systems that are utilized by employees all over the world, they are subject to a specific set of data regulations in each country such as ITAR, and Europe's Data Protection Compliance regulations. Using a cloud backup provider locked to a single geography is not only inefficient but, in many cases, results in a violation of fast-evolving local data residency laws.

By contrast, leading cloud backup providers are equipped with multiple redundant data centers across the globe, enabling customers to control which data centers are used for their data backups to ensure compliance with local data regulations. With elastic, on-demand storage, customers can add storage instantly in any data center without having to worry about scaling their storage requirements.



Benefit from large-scale cloud computing platforms like Amazon Web Services

Cloud service providers who leverage a cloud computing service like Amazon Web Services can provide customers with features beyond what they would be able to if they developed their own platform – such as on-demand storage scalability, instant provisioning, and access to data centers across the globe. Customers benefit from the ability to use the massive cloud infrastructure that serves always-on businesses like Amazon, Netflix, Expedia, and Adobe.

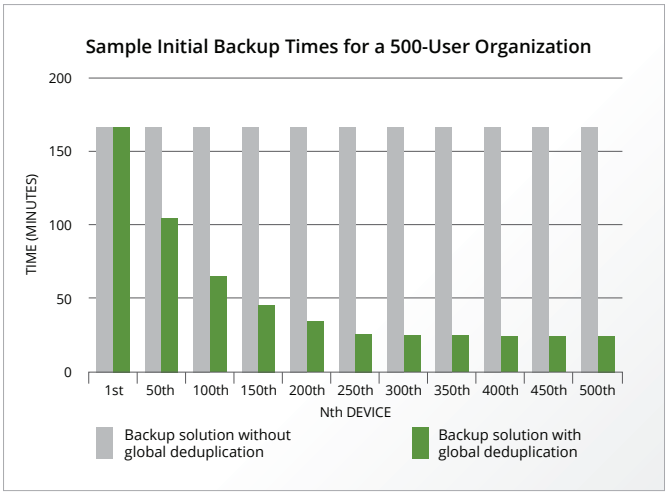
4. High-performance backups

One of the realities about cloud backup is that it can be painfully slow--laptops store gigabytes of data that must be transferred to the cloud, often over weak wifi networks. Fortunately, it doesn't have to be that way - cloud backup services can employ a number of effective tactics to significantly speed up backups by reducing the amount of data to be transferred and making optimal use of available bandwidth:

Global Deduplication: Given that as much as 80 percent of data is duplicated across a typical enterprise, cloud backup software can significantly speed up backups by eliminating data redundancy across all devices in an enterprise and only saving a single instance to the cloud.

WAN Optimization: Administrator level parameters that can be set by policy to manage both bandwidth allocated to the backup service and the amount of client resource allocated to processing the client side assessment.

Caching: For the best performance both server-side and client-side, caching should be employed to reduce processing overhead. The addition of an on-premise caching solution can take this one step further by enabling fast onsite transfer of data via LAN to the caching server, then transferring the data from the caching server to the cloud via WAN.



5. Extend backup to data governance

Ideally, any investment you make in a cloud backup provider is the first step in a larger data protection and governance strategy. Cloud backup solutions that go beyond simple backup to provide new ways to increase IT visibility and control over endpoint data are worth a closer look.

One example of this is leveraging data stored in the cloud for eDiscovery, enabling IT to quickly locate information on any device, enforce data usage policies , and preserve data. Such a solution can bring tremendous cost savings to companies who need to respond to legal requests, freeing up vital IT resources from labor-intensive, costly data collection for other critical IT projects.

Visibility & Control Checklist

- *Audit trails for users and admins*
- *Federated search*
- *Granular policies for backup, access, restore, and sharing*
- *Legal hold to preserve-in-place*
- *Integration with eDiscovery solution*

Key features of an eDiscovery offering include detailed audit trails, which serve as a record of all user and admin activity and provide real-time visibility, enabling organizations to support their governance and compliance needs. In addition, federated search can enable IT to locate files across every device in the enterprise, and built-in legal hold makes it easy identify custodians and gather data for eDiscovery.

For enterprises subject to industry regulation, it's important to select a service provider that already has passed the requisite certifications (e.g., HIPAA, PCI-DSS, ITAR) for its data centers and operations.

Consider your cloud backup provider choice as the first steps in a cloud-based data governance policy that can scale.

HIPAA Compliance

Over 750,000 individuals' PHI breaches took place in the first six months of 2014 alone. Ensure that the cloud is audited to validate its security and privacy controls for handling HIPAA-compliant PHI. This ensures all levels of the technology stack IaaS, PaaS and SaaS meet the guidelines required by HIPAA/HITECH.

Conclusion

For enterprises looking to protect the corporate data on their employees' endpoints, there are significant business benefits to moving to a cloud-based backup provider. Yet, all providers are not the same. Being mindful of the differences can save you headache and set your business up for cost savings, increased security and the ability to respond to new business demands. Select a solution that ensures security, uptime and scale, as well as the ability to move beyond simply data backup.

To aid you in your consideration, we've created the following checklist to use when evaluating cloud-based backup solutions:

5-Point Checklist for Considering Enterprise Cloud Backup Providers

- ☑ Limit your search to one that is certified compliant with international standards such as SOC 1 and ISAE 3000 Type II to MMMM to ensure top level security.
- ☑ Understand service level agreements (SLAs) to ensure continuous service availability and data integrity that meet the industry standard of 99.5% uptime.
- ☑ Pick a cloud provider equipped with multiple redundant data centers across the globe, enabling customers to control which data centers are used for their data backups to ensure compliance with local data regulations.
- ☑ Ensure zero impact to end users by picking a solution provider that offers the fastest backups possible to reduce the amount of data transferred and make optimal use of available bandwidth.
- ☑ To go beyond simple backup and extend to eDiscovery, select a service provider that already has passed the requisite certifications (e.g., HIPAA, PCI-DSS, ITAR) for its data centers and operations.

More Resources

Visit Druva.com/resources for additional resources for learning more about endpoint backup.

[The Essential Security Checklist for Enterprise Endpoint Backup]

[8 Must-Have Features for Endpoint Backup]

[Gartner evaluates leading endpoint backup providers]

About Druva

Druva is the leader in converged data protection, bringing data-center class availability and governance to the mobile and distributed enterprise. With a single dashboard for backup, availability and governance, Druva's award-winning solutions minimize network impact and are transparent to users. As the industry's fastest growing data protection provider, Druva is trusted by over 3,000 global organizations on over 3 million devices. Learn more at **www.druva.com** and join the conversation at **twitter.com/druvainc**.

druva

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44.(0)20.3150.1722
APJ: +919886120215
sales@druva.com
www.druva.com

Q117-CON-10592