



What is cloud-based backup and recovery?

Executive Summary

Companies struggle with the challenges of effective backup and recovery. Small businesses lack dedicated IT resources to achieve and manage a comprehensive data protection platform, and enterprise firms often lack the budget and resources for implementing truly comprehensive data protection.

“Cloud-based backup and recovery lets companies lower their data protection cost or expand their capabilities without raising costs or administrative overhead.”

Cloud-based backup and recovery lets companies lower their data protection cost or expand their capabilities without raising costs or administrative overhead. Firms of all sizes can benefit from cloud-based backup and recovery by eliminating on-premises hardware and software infrastructure for data protection, and simplifying their backup administration, making it something every company should consider.

Partial or total cloud backup is a good fit for most companies given not only its cost-effectiveness, but also its utility. Many cloud-based backup vendors offer continuous snapshots of virtual machines, applications, and changed data. Some offer recovery capabilities for business-critical applications such as Microsoft Office 365. Others also offer data management features such as analytics, eDiscovery and regulatory compliance.

This report describes the history of cloud-based backup and recovery, its features and capabilities, and recommendations for companies considering a cloud-based data protection solution.

What does “backup and recovery” mean?

There's a difference between “backup and recovery” and “disaster recovery.” Backup and recovery refers to automated, regular file storage that enables data recovery and restoration following a loss. Disaster recovery refers to restoring not only lost data, but also infrastructure component configurations, and application data and database contents, back to a specific time or functionality. Typically, this involves restoring applications and components as they were just before the disaster event, whether natural disaster, cyber attack, hardware failure, or human error.

“Business continuity” is the next step beyond disaster recovery. It refers to restoring other elements of business operations that can be affected by catastrophic data loss. For example, if a flood or hurricane knocked out power to the data center and IT operations were down, IT infrastructure and applications would need to be restored, and employees would need to continue doing their jobs even if they were unable to report to work or access critical IT resources. Business continuity protection can enable work-from-home options, backup telephone systems, and payroll processing.

Robust capabilities at low cost

Until recently disaster recovery (DR) has been prohibitively expensive for most small and medium-sized businesses, requiring duplicate on-premises infrastructure for DR. In the past five years, however, cloud-based backup and recovery vendors have introduced sophisticated data protection capabilities to firms of all sizes at an affordable cost. Even large enterprise companies that are used to spending heavily on data protection can now realize significant savings compared to on-premises backup via tape and/or redundant disk-based backup for data centers and individual computers.

Despite the affordable cost, most SMBs have inadequate backup procedures or none at all. Managing complex backup strategies such as rotating tapes to offsite storage has often been a full-time job, one that typically received little attention until a data loss.

As backup costs have gone down, capabilities have gone up. Some companies have taken the opportunity to keep

“Cloud-based backup and recovery is making the decision to protect even end-user data much easier.”

their backup and recovery budgets static while improving their data protection capabilities. Enterprise firms, recognizing how devastating data losses can be to operations, have always been more willing to spend whatever it took to protect their data. However, many enterprise IT departments have not backed up end-user data due to the cost and complexity of managing backups and frequent requests to restore lost data. Cloud-based backup and recovery is making the decision to protect even end-user data much easier.

Benefits of cloud-based backup and recovery

Here are some of the benefits of a cloud-based backup and recovery solution:

Lower TCO: Cloud-based data protection can significantly reduce the total cost of data backup infrastructure. Along with lower licensing costs and fewer expensive on-premises storage arrays, cloud backup and restore means less administration time and reduced demands on help-desk staff.

Ability to protect more data: Lower cost cloud-based data protection gives companies that cannot afford on-premises data protection an affordable alternative. Companies can now protect end user data, non-production server data, and other data repositories that were unprotected or inadequately protected previously.

Self-service backup/restore: Cloud-based backup and restore is accessible to end users, making it viable for any size company. End user restores have always been extremely time consuming for help desks and backup admins. Cloud-based backup and restore lets users customize their backups and restore data on demand.

Reliable, hands-off backup: Once configured, cloud-based backups continue on schedule indefinitely, allowing backup admins to focus on higher-value activities.

Auto-scaling backup resources: As data volumes continue to grow, cloud-based backup and restore means that a backup vendor takes care of scaling, availability, and redundancy of cloud resources. Also, some cloud-storage vendors charge based on the amount of data backed up. Companies save by paying only for what they use, versus provisioning their own on-premises storage arrays. On-premises arrays are underutilized until the moment when they become oversubscribed, at which point more expensive storage resources must be purchased and implemented.

Automated offsite backup: Cloud-based data protection offers offsite data storage as part of the architecture. Some vendors replicate data to multiple clouds, providing offsite replication in addition to storage, and an additional layer of data protection.

Phased implementation: Moving to cloud-based backup does not have to happen all at once. Phased implementations are much easier than hard deadlines. The customer controls the schedule and which data has priority.

Cloud-based or cloud-native backup?

There is a difference between backup vendors that offer cloud-based vs. cloud-native backup and recovery, usually centered around how the product was originally architected. Cloud-based is generally sold as a customer managed product, including software and possible on-site hardware appliances. Cloud-native backup and recovery is offered as-a-Service, with the customer only deploying backup agents in the devices to be protected. The SaaS vendor maintains the backup infrastructure in the cloud, offering subscription based pricing for their services.

“Cloud-native backup and recovery is offered as-a-Service, with the customer only deploying backup agents in the devices to be protected.”

A cloud-based backup and recovery strategy can include components such as a software “agent” on the computers being protected, a backup appliance, and, in hybrid scenarios, local storage that caches cloud-bound data or serves as an on-premises repository for backups. It’s a good idea to evaluate vendors’ agent technology to ensure that it provides necessary capabilities without burdening protected computers with CPU and/or memory-intensive software.

Some vendors may supplement their cloud-backup capabilities with a local backup appliance, which often include capabilities such as caching cloud-bound data, encrypting data, and facilitating the management of backup and restore processes, locally and in the cloud. Depending on the backup vendor's appliance's capabilities, it may also be possible to configure appliances to attach to multiple clouds, appliances in other locations, or local storage in hybrid-cloud architectures.


For vendors supporting creation of a baseline backup that can be burned to disk then mailed in to the vendor to seed initial backups more quickly, a local appliance provides the initial backup process and creation of the backup set that can be burned and mailed.

Use cases

With its low cost and ease of use, cloud-based backup and recovery works well with wide-ranging data protection scenarios. This section describes several use cases.

Servers

- **SMBs** – Servers are a prime cloud-based backup and recovery application for SMBs, which are often challenged by the cost and complexity of protecting server data. Installing an agent on a server is relatively easy, and once it's installed, it can be configured from a centralized management console for backup frequency and data storage location. Smaller servers may not even need a backup appliance; server agents can back up to and restore from the cloud directly. The self-service nature of cloud-based backup and recovery also makes it convenient for SMBs given the expense of dedicated IT staff for server backups.
- **Enterprises** – Most enterprise companies have sophisticated backup and recovery procedures in place for production servers. However, enterprises often don't prioritize regular backups for nonproduction servers, including development and test servers. Low-cost cloud-based backup and recovery is an attractive choice in this situation. Cloud backups can save hours or days of reconfiguring non-production servers in the event of data loss. Self-service cloud backups are also attractive to developers and operations personnel managing nonproduction servers.



“Cloud-based backup and recovery works well with wide-ranging data protection scenarios.”

Self-service backups and restores

Low cost and ease-of-use make self-service data protection a natural fit for SMBs and enterprise-size businesses alike.

- **SMBs** – Self-service backup and restore is ideal for SMBs given the low likelihood of dedicated staff for managing backups. Hence, self-service cloud-based backup and recovery is practically an operational requirement to ensure that business operations continue in a timely fashion after a data loss.
- **Enterprises** – For some enterprises, backing-up end-user data is too costly and complex to justify protecting company-wide. Low-cost, easy-to-use self-service backup-and-restore capability allows enterprises to protect data they can't or won't protect globally.

Archive in the cloud


The cloud's vast scalability and end-user management choices make cloud backup and restore an excellent choice for archive storage. End-users should evaluate entry costs and data access times when using cloud-storage services such as Amazon Glacier, or look for a vendor that uses policy-based auto-tiering to move data to cold storage. Amazon Glacier, for example, can take hours for retrieval so should be limited to cold, infrequently accessed data. Many MSPs offer archival-storage-as-a-service in their own clouds or in environments hosted on Amazon, Glacier, Azure, Rackspace, and others.

Remote office/branch office

Remote office and branch office (ROBO) use cases are perfect for cloud-based backup and recovery. Cloud-based backup solutions manage backup and recovery from a centralized management console, enabling IT can configure backups and restore files from cloud-based backups with no intervention from onsite personnel. ROBO operations need comprehensive remote management features, allowing management tasks to be completed over the network instead of requiring onsite management.

Disaster recovery

Disaster recovery (DR) is another strong use case for cloud-based backup and recovery. Many DR solutions allow the backed-up image to be booted directly in the cloud, so that operations can continue. The backup and recovery appliance can boot-up virtual servers quickly, ensuring continuity of operations while the problem is being addressed. Not all backup and recovery solutions support these DR features, and so companies should determine whether these capabilities are important.



Low cost and ease-of-use make self-service data protection a natural fit for SMBs and enterprise-size businesses.”

Workload mobility

Cloud-based backup and recovery can also enhance workload mobility, allowing organizations to replicate quickly and create instances in the cloud for testing and development or for moving workloads to different cloud regions to optimize accessibility, continuity, or data residency. With data no longer tied to hardware, businesses can replicate and migrate easily.

Governance

Over the past 10 years corporate governance and compliance have become business-critical for most companies. The IRS requires financial data to be retained for at least seven years, and other regulations, such as FINRA and Sarbanes-Oxley, have even longer horizons. Regulations such as HIPAA have stringent requirements for securing personally identifiable information (PII), which means that companies need backup and recovery capability that supports strong encryption and data security. Considering stringent governance and compliance regulations, the cost of a robust backup and restore solution is easy to justify.

Best practices for implementing cloud-based backup and recovery

Some best practices for evaluating and implementing a cloud-based backup and restore strategy are common to most types of IT projects. However, there are situations and techniques that are unique to cloud-based data protection projects. Here are the most important things to keep in mind when implementing cloud-based data protection software and hardware.

Planning: *“Fail to plan, plan to fail.”* Always have a project plan in place to guide evaluation, procurement, implementation, and support of your cloud-based backup-and-restore strategy. Even an informal document is better than none at all. Outline who’s responsible for the various aspects of a successful implementation, what happens when something goes wrong, and how and where users can get backup-and-restore support.

Architecture: Cloud-based data protection can run on a variety of architectures, including direct-to-cloud, hybrid-with-caching, hybrid-with-storage, and local-appliance-to-cloud. Here are descriptions of each option:

- **Direct-to-cloud** – For those ready for cloud-native backup and recovery, you can deploy data protection agents that communicate directly with cloud backup resources to ensure uninterrupted data flow to and from the cloud. These agents don’t need a local appliance to access cloud resources and coordinate backup and restore. Advantages include lower cost-of-ownership, given no need for a local appliance, and simple architecture. Look for vendors that offer a centralized management console for all backup operations, including managing the backup data in the cloud.
- **Hybrid with local caching** – Hybrid architectures with local caching require a local appliance with sufficient memory and disk resources to cache cloud-bound data. If network bandwidth between the appliance and the cloud becomes restricted or overloaded, the appliance caches the data locally and uploads it to the cloud when bandwidth becomes available. The cached data is deleted from the local appliance after uploading.

- **Hybrid with local storage and cloud archiving** – Another hybrid cloud-archiving scenario uses a local appliance with storage. This architecture enables data tiering based on user-defined criteria, e.g., age of file, last access date, access frequency, and business-critical or performance characteristics. Not all vendors support this scenario, and those that do offer a variety of configurations and options for tiering your data exactly as required. The downside of this implementation is the higher cost of ownership for maintaining on-premises backup capacity.

Testing: Testing all of your potential cloud-based data protection solution choices thoroughly helps minimize surprises during the implementation and operational phases. IT should test each product's backup-and-restore processes, and if you're implementing server backup-and-restore capabilities, be sure to include server-and-backup admins in the evaluation and testing phases.

Encryption: Data security is just as important to your company's success as adequate backup, so be sure that the products you evaluate include appropriate encryption. This is an absolute necessity in industries that are subject to data security and privacy regulations, such as HIPAA, FINRA, and Sarbanes-Oxley. Be sure that the cloud-based solutions you evaluate include appropriate encryption levels (both in-transit and at-rest) and sufficient data security features to ensure compliance with all applicable regulations and company guidelines.

Seeding backups: Most cloud-based backup-and-restore vendors can make an initial full-server backup that would take too long to upload to the cloud via a WAN-connected local appliance. However, the initial full backup can often be captured and burned to disk via separate utility, or the appliance might include that capability. Then you can send the backup disks to your vendor for uploading to the cloud, followed by all future incremental backups. This saves days or even weeks of uploading to achieve the initial backup. Seeded backups for end-user computers are usually less critical as they're likely to have much less data than servers. However, if any of your end users have large amounts of business-critical data stored locally, you can always opt to seed their initial backups via disk just as you would a server.

Cloud-backup redundancy: Along with tiering data between local and cloud storage, some cloud-based data protection vendors also let you replicate backup data among other data centers and among multiple clouds. Some local appliances in company-owned data centers can replicate data among multiple data centers—with a similar appliance in each—to give you geographic backup-data redundancy. Some vendors also enable connecting one appliance to multiple cloud instances, to replicate business-critical data across a variety of locations.

“If your company is not taking advantage of cloud-based backup and recovery, there is no time like right now to implement a suitable solution.”

Support: Even the best cloud-based data protection is worthless if the vendor is not available to provide help in a timely manner to the project manager or operational IT manager. We recommend testing each vendor's support processes and expertise as part of your product evaluations. Online knowledge bases and robust support portals are extremely useful, but you still need to be able to reach a real support agent quickly, who has the expertise to fix your problem—or find someone who can.

Be sure to test vendors' customer support mechanisms, not relying on the usual handholding from a pre-sales engineer. Once you commit to a solution, you need to know that the company will be there to help when you need it.

Why it matters

Cloud-based backup and restore is revolutionizing data protection. It has become a compelling value proposition for every company looking to prevent potentially catastrophic data loss, from SMBs to corporate enterprises and everything in-between. Cloud-based backup and recovery is the obvious solution to expensive conventional enterprise data protection schemes, and it's also very useful for typically unprotected smaller firms with limited budgets.

Industry experts estimate that more than 70 percent of businesses hit by significant data loss go out of business within 18 months—we saw this type of impact to local businesses after the 9/11 attacks. Hence, data protection has gone from an expensive wish-list item to a budget-friendly, solution that's critical to your company's ongoing operations.

If your company is not taking advantage of cloud-based backup and recovery, there is no time like right now to implement a suitable solution. The survival of your company could be at stake. If your company has a data protection strategy in place, you can still explore the cost-saving potential of cloud-based backup and recovery or increase your data protection capabilities without increasing costs, or, in some cases, both. We recommend exploring the potential of cloud-based data protection and look into determining how these capabilities can help you better protect your business-critical data. The question is no longer whether you can afford it, but rather, can you afford not to?

Check out druva.com/cloud-backup and see how you can take advantage of cloud-based backup and recovery.



Find Druva in AWS Marketplace

Get Started



Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976

Europe: +44 (0) 20-3750-9440

India: +91 (0) 20 6726-3300

Japan: +81-3-6890-8667

Singapore: +65 3158-4985

Australia: +61 1300-312-729

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital, Viking Global Investors, and Nexus Partners. Visit [Druva](https://druva.com) and follow us [@druvainc](https://twitter.com/druvainc).