

Managing the information that drives the enterprise

STORAGE

essential guide

CLOUD BACKUP AND CLOUD DISASTER RECOVERY

Cloud backup and DR are now viable alternatives for enterprise data protection environments.

Hybrid approaches can effectively integrate on-premises systems with cloud storage services.

ALSO ■ CLOUD BACKUP BENEFITS ■ ENTERPRISE CLOUD BACKUP
■ HYBRID CLOUD BACKUP ■ CLOUD-BASED DR BLUEPRINT ■ REMOTE CLOUD BACKUPS



editorial * rich castagna

Benefits of cloud backup and DR become more apparent

Cloud storage services for backup and DR have been around for a while, but new products and evolving technologies now make them viable alternatives for enterprise storage shops.

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups

STORAGE MANAGERS HAVE long been attracted to the economic benefits of cloud storage. You don't have to buy stuff like hardware and software, and you only pay for the storage capacity that you actually use. With no capex and little opex, what's not to like? Well, bandwidth, security and data restoration were a few of the answers to that question, and were easily among the top barriers to enterprises looking to tap into cloud storage. Integrating cloud storage into an existing storage environment was another serious concern and, lacking effective integration, having to manage isolated—and distant—silos of data.

But that was then, and this is now: cloud storage vendors, hardware vendors and software vendors have all made great strides in

the last few years with products and services that address most of those concerns more than adequately.

WAN optimization hardware and software, along with data reduction techniques, help reduce the amount of data that actually has to flow from the data center to the cloud storage service. This makes it easier to treat cloud storage as just another storage tier. Backup apps that do their own deduping and can access the cloud as if it were just a NAS target have also made it easy to deploy cloud storage without having to revamp backup operations.

Hybrid cloud storage products adroitly bridge local and online sites to preserve the benefits of on-premises and cloud storage seamlessly. You can send your data to an on-site appliance where it remains available for a specified period before it loses its urgency and gets shipped to the cloud. This, too, is as close to painless as cloud storage integration gets.

The cloud storage providers themselves have evolved significantly and now offer services that just a few short years ago were out of the reach of all but the wealthiest of companies. A good example of this is cloud disaster recovery. With cloud DR, your data is replicated regularly to the cloud site to ensure that there's a full, duplicate copy stashed safely offsite. When a disaster occurs, the cloud DR provider can spin up some virtual servers that can access your apps and data and put you back in business in a matter of hours.

As it matures, cloud storage becomes more and more useful and a much better fit for enterprise and SMB storage environments. And the ability to incorporate these services almost effortlessly makes them an even better bargain. In this Essential Guide, we'll get you up to speed on modern cloud storage services and suggest some ways you can use them at your company to improve storage operations. ■

[Rich Castagna](#) is editorial director of the Storage Media Group.

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups

Cloud backup is ready for the enterprise

Cloud backup services have seen increased adoption by SMBs, but with a choice of methods and tighter controls, cloud backup is now also a viable enterprise alternative. BY JACOB GSOEDL

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups

BACKUP WAS ONE of the first services offered by cloud storage vendors, and it's still the most popular way of using cloud storage. Once considered an option for only smaller companies, some enterprises are now using cloud backup for remote office and desktop/laptop data protection, archival and off-siting of backups to supplement existing in-house backup services.

The benefits of backing up to the cloud are compelling: no need for backup infrastructure, minimal IT resource requirements and usage-based pricing that becomes part of your monthly operational expenses. But the benefits are offset by security concerns and restore challenges, especially if a lot of data must be restored from the cloud. With accelerated adoption of cloud services, cloud-based backup options have substantially increased, giving companies several alternatives:

- Backup managed service providers (MSPs)
- Cloud-enabled backup applications
- Cloud gateways

CLOUD CONSIDERATIONS

Regardless of the alternative your company opts for, this list of key features and considerations will help determine the right product for your environment.

Security. Security is still the main reason companies steer clear of cloud services. To address security concerns, cloud backup products must adhere to the minimum following best practices:

- Data must be encrypted during transit, usually via a secure socket layer (SSL) connection if the Internet is the transport
- Data must be stored encrypted in the cloud via a state-of-the-art encryption protocol, such as 256-bit AES encryption
- The cloud service provider must support strong, enforceable authentication with features like password expiration and complexity

Encryption key management must be clearly understood; most cloud service providers defer key management to users with the benefit that encryption keys are unavailable within the cloud. But with encryption key management the responsibility of users, the cloud service provider won't be able to help if the keys are mismanaged or lost, preventing access to the data. Because encryption keys are critical, some companies put them in an escrow account as protection against loss or corruption.

Compliance. There may also be compliance issues related to using cloud backup. For public companies or industries that are subject to additional regulatory requirements, only cloud service providers that adhere to SSAE 16/SOC 1 (formerly known as SAS 70) should be considered. SAS 70/SSAE 16 is an audit standard for service providers where an external auditor evaluates controls and processes, and prepares a report that's shared with the service

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups

provider's customers. Because there's a Type I and Type II SAS 70/SSAE 16 examination, it's crucial to confirm that the service provider performs the more stringent Type II audit. Only a Type II audit report expresses the auditor's opinion on whether the controls tested operated effectively enough to provide reasonable assurance that the control objectives were achieved during the period specified. For instance, Sarbanes-Oxley (SOX) audits usually only rely on Type II audit reports.

You should also understand the scope of the audit report and what it covers. Many smaller MSPs are quick to declare SAS 70/SSAE 16 compliance by providing data center or Amazon (if the MSP uses Amazon on the back-end) SAS 70/SSAE 16 reports, which usually aren't sufficient. While a data center SAS 70/SSAE 16 report addresses physical controls, it has no bearing on operational controls of the MSP in relation to change management, program development and access grants. Therefore, it's highly recommended to request the latest SAS 70/SSAE 16 report from the cloud service provider prior to signing with the service, and to have the report reviewed by the internal and external auditors.

Hybrid vs. pure cloud backups. In a pure cloud backup scenario, agents on protected servers and desktops perform backups directly to the cloud. Quick setup and minimal maintenance are benefits of this service. A pure cloud backup product is best suited for personal backups and backups for smaller firms with limited amounts of data to protect (typically a few terabytes). The drawbacks of backing up directly into the cloud are performance and bandwidth challenges because of latency and bandwidth limits of available Internet connections; these shortcomings are most important when restoring data.

Latency and limited bandwidth are mitigated by hybrid cloud backup products that use an on-premises disk or gateway as the initial backup target from which the data is replicated to the cloud.

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups

- Cloud backup benefits
- Enterprise cloud backup
- Hybrid cloud backup
- Cloud-based DR blueprint
- Remote cloud backups

The on-premises intermediary usually caches the most recent backups for on-premises restores, minimizing tedious recoveries from the cloud; it also moves data into the cloud asynchronously. For a pure cloud backup solution without the on-premises intermediary for quick restores, it's essential to understand all restore options, including the ability to have backups shipped to you on a disk or NAS device; restore options become more relevant as the amount of data stored in the cloud grows. Similarly, some MSPs accept the initial full backup on an external storage device (known as "seeding") to avoid a time-consuming first backup over the Internet.

Cloud backup options: The pros and cons		
OPTION	PROS	CONS
Managed service provider (MSP)	• Simplicity • Cost-effective • Few on-premises IT resource requirements	• Complete dependency on the MSP for all aspects of the backup • Control is handed off to the MSP
Cloud-enabled backup applications	• Extends and supplements existing backup infrastructure and processes • Except for backup data location, control remains with the customer • Cost-effective	• Requires a cloud-enabled backup application • Little impact on IT resource requirements
Cloud gateways	• Works with any backup application that supports backup to disks • Extends and supplements existing backup infrastructure and processes • Except for backup data location, control remains with the customer	• Introduction of an additional IT infrastructure component that needs to be managed • Higher cost

Efficiency. Backup processes that are OK for on-premises backups may be unacceptable for cloud backups. For instance, the ability to perform sub-file backups of changes to files is an indispensable feature in a cloud backup product. With email personal folder files (.PST files) that can grow beyond gigabytes, and large Excel spreadsheets and PowerPoint presentations spanning tens of megabytes, being able to only back up file changes to the cloud rather than complete files is a non-negotiable feature for a cloud backup product. Similarly, the ability to perform continuous incremental backups minimizes the amount of traffic for each backup. The traditional weekly full and daily incremental backup discipline frequently used for on-premises backups doesn't work for backing up data into the cloud. Limited network bandwidth makes efficiency one of the primary virtues in a cloud backup product. So anything that can help reduce the amount of data to be moved into the cloud is critical.

Limited network bandwidth makes efficiency one of the primary virtues in a cloud backup product.

Compression and source-side dedupe are two approaches that help minimize the amount of traffic sent into the cloud. Data deduplication reduces bandwidth usage and also helps cut the cost of backing up to the cloud. Because cloud storage pricing is usually based on gigabytes stored, compression and dedupe are instrumental in lowering monthly fees. To maximize data reduction, some MSPs deduplicate on the source side and one more time in the cloud. While the scope of source-side dedupe may be limited to a single or few hosts, dedupe in the cloud can be performed against all data, resulting in significant additional data reduction.

“We deduplicate and compress before we send data across, and we deduplicate one more time once data is in the cloud,” said Kar-

en Jaworski, senior director of product marketing at EVault (formerly i365), a Seagate company and backup MSP.

Transport. Besides source-side dedupe, cloud backup products differ in the way they manage available bandwidth. The ability to limit and throttle bandwidth while backups are in progress helps minimize the impact on users and other apps sharing the Internet connection. Moreover, being able to configure multiple bandwidth limits for different times of the day helps optimize the balance between backup performance and the impact on other users. Some cloud service providers, such as AT&T, give customers the option to use a multiprotocol label switching (MPLS) circuit instead of the Internet; this option is relatively cost-effective for customers who already use MPLS. The quality of service (QoS) feature of MPLS lets users label backup data as low-priority traffic, eliminating the impact on other users and applications altogether. This is especially attractive for midsized and large companies with many users and a lot of protected data.

BACKUP MANAGED SERVICE PROVIDERS

Handing off backups to a managed service provider is the quickest way of getting backups into the cloud and the method with the fewest internal IT requirements. MSP offerings are available as pure cloud backup products where the user installs agents on desktops and servers that directly back up data into the cloud; they're also available as hybrid cloud backup products where the cloud service vendor provides a managed on-premises gateway to store backup data locally before replication into the cloud.

MSP offerings range from consumer, small office/home office (SOHO) and small- and medium-sized business (SMB) products to cloud backup services targeted at the enterprise. "While the sweet spot for cloud-based backup is still the small to midsized company,

larger enterprises have started leveraging the cloud to supplement internal backups, especially for DR [disaster recovery], remote office and end-user data protection,” said David Chapa, formerly a senior analyst at Milford, Mass.-based Enterprise Strategy Group (ESG).

Consumer backup services were popularized by Mozy (now part of EMC Corp.) and Carbonite. They’re pure cloud backup products, licensed to protect a single desktop or laptop, and may not have all the features expected in a business backup product. For instance, the Carbonite service doesn’t offer deduplication. “Deduplication is less required in our target market where the average amount of protected data is less than 50 GB,” said Pete Lamson, senior vice president and general manager of Carbonite’s Small Business Group. Both Carbonite (with Carbonite Business) and Mozy (with MozyPro) have expanded their offerings into businesses. While Carbonite targets small businesses with a simple and highly affordable backup service, MozyPro is aimed at small and large businesses alike.

Joining Carbonite with a focus on small companies with up to 50 users is Symantec Corp. with Backup Exec.cloud. “Backup Exec.cloud has centralized management and provides global visibility to protected hosts, and we try to make backup as simple as possible,” said David Mitchell, product manager for Symantec’s hosted endpoint protection.

For enterprises, IBM has rebranded and renamed its managed backup service offerings with a focus on resilience: SmartCloud Resilience. The IBM product spans the data protection spectrum from backup and recovery to archival and DR.

EVault has been offering managed backups since 1997, and the company has one of the most complete and feature-rich cloud backup offerings addressing the needs of small and large companies. Available as pure service, software, and physical and virtual appliances, it can be deployed on-premises, in a hybrid arrangement or as a pure cloud backup product.

Iron Mountain Inc. has one of the strongest brands in the backup world but its cloud message changed with the sale of its Connected Backup and LiveVault backup software to Autonomy (Autonomy is now part of Hewlett-Packard). Iron Mountain is currently focusing on backup services rather than software development.

“We continue to offer cloud backup services for businesses,” said Ken Rubin, senior vice president and general manager of the Iron Mountain healthcare service. “For the healthcare and financial services sectors, we provide advanced solutions; for instance, for hospitals we offer a managed backup product with tight integration with all major PACS [picture and archival communication system] systems.”

CLOUD-ENABLED BACKUP APPS AND GATEWAYS

While small companies are more likely to opt for the MSP approach, larger companies are more apt to extend their existing backup infrastructure into the cloud using either their existing backup software or a cloud gateway. The incentives to expand the backup infrastructure into the cloud range from replacing off-site tapes with backups in the cloud to leveraging the cloud for backup jobs that can be performed more cost-effectively.

Cloud support in commercial backup applications varies considerably. CommVault Systems Inc. has added extensive cloud support and supports a wide range of cloud service providers (AT&T, Amazon, Microsoft, Nirvanix and Rackspace). Supported cloud providers appear as additional backup media and all backup features, such as deduplication, are available when backing up to the cloud. Archival into the cloud with stub support for on-demand retrieval of archived data and block-based replication of changes into the cloud for recovery into a compute cloud service such as Amazon Elastic Compute Cloud (EC2) are just a couple of features that distinguish CommVault Simpana. Similar to CommVault, both Symantec

tec Backup Exec and NetBackup support backing up into the cloud; they currently support Nirvanix, Amazon Web Services (AWS), Rackspace and AT&T. Arkeia Network Backup supports replication of backup sets into Amazon and Nirvanix.

EMC Avamar and NetWorker currently don't have out-of-the-box integration with cloud service providers. Instead, EMC is selling Avamar to MSPs. "We decided on Avamar to power our enterprise backup service because of its efficient source-side deduplication and scalable Avamar Data Store grid," said Dick Mulvihill, co-founder and managing partner at Hexistor Data Protection Service LLC, a Chicago-based backup MSP.

Cloud backup checklist: Key features

FEATURE

REASON FOR RELEVANCE

Encryption of data in transit and at rest in the cloud

Prevents access to the data by cloud service provider staff and other unauthorized users

SAS 70/SSAE16 Type II compliance of the cloud service provider

Ensures the service provider has strong IT controls in place; a must-have for public companies and for industries with additional regulatory requirements

Data deduplication

Reduces storage cost; source-side deduplication also reduces bandwidth requirements

Hybrid cloud backup option

Cached on-premises backups eliminate long restore times of a pure cloud backup solution

Getting data in and out of the cloud via physical device

Options of initial "seeding" of backups and delivery of restore data via physical disk to minimize initial backup and restore times

Incremental forever

Ensures efficient ongoing backups

Sub-file-level backup of changed files

Minimizes the amounts of data to be backed up, especially with large files

Bandwidth features

Throttling and scheduling to minimize the impact of backups on other users

IBM Tivoli Storage Manager (TSM) doesn't currently support direct backups into the cloud. "We're working with cloud gateway manufacturers such as Riverbed for cloud backup support; cloud backup gateways are simple and quick to set up and have the advantage of locally cached backups for quick restores," said Steve Wojtowecz, vice president of storage software development at Tivoli.

Cloud gateways that move data into cloud storage are available from Nasuni Corp., Panzura Inc., Riverbed Technology Inc., StorSimple Inc., TwinStrata Inc., and others. While some gateways are touted as hybrid cloud storage products to extend on-premises storage into the cloud, Riverbed Whitewater's focus is exclusively on cloud backup. Available in different configurations for small businesses to large enterprises, traditional backup applications back up to the Whitewater gateway appliance, which then deduplicates, compresses, encrypts and asynchronously moves data into supported cloud providers (which currently include AT&T, Amazon and Nirvanix). The StorSimple gateway stands out because of its extensive support of Microsoft SharePoint.

CLOUD BACKUP GOES MAINSTREAM

Backup to the cloud is moving from a niche application into the mainstream, especially in the SOHO and SMB sectors, and it's being used increasingly by larger companies to supplement their existing backup infrastructure. The increased adoption of cloud services by public companies and even government agencies suggests that security concerns with cloud services are slowly abating. However, proper due diligence must be taken when evaluating cloud backup, such as implementing solid backup processes and strong controls, to avoid unpleasant surprises. ■

Jacob Gsoedl is a freelance writer and a corporate director for business systems.

Hybrid cloud backup: Disk-to-disk-to-cloud backup explained

Cloud storage services are viable alternatives to tape for companies that back up to disk but need to retain backup data for longer periods. BY RACHEL DINES

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups

DISK-TO-DISK-TO-CLOUD backup is gaining in popularity in both large enterprises and small businesses. Similar in concept to disk-to-disk-to-tape (D2D2T), in disk-to-disk-to-cloud backup, users first back up their data to a disk, and then transfer it to the cloud. Although it is often faster and more convenient to backup to the cloud, this hybrid cloud approach to backup may or may not be right for your organization.

Rachel Dines, an analyst at Forrester Research, discusses the pros and cons of disk-to-disk-to-cloud backup and hybrid cloud backup approaches in this Q&A.

What would a typical disk-to-disk-to-cloud backup scenario look like?

There are actually two ways that I see disk-to-disk-to-cloud deployed. The first way is a traditional on-premises backup deployment with whatever enterprise or small- to medium-sized business (SMB) backup solution you have, whether it's with CA,

CommVault, IBM Tivoli Storage Manager (TSM) or Symantec Corp. You would back up your data locally and then take your local backup to disk, and replicate that to the cloud as if it were any tertiary medium like tape. So that's very well integrated with what you have today. It's not really a huge departure or radically different from what we're used to with disk-to-disk-to-tape, which is a very common setup.

Another disk-to-disk-to-cloud deployment model that I do see is a managed appliance from the provider where they put an appliance onsite; in this case, it would be more like a backup-as-a-service, except you would still be backing up locally to an appliance and then replicating to a cloud. The main difference is that you're not managing the software at all. You're not managing the appliance. That's all done by the provider.

Have you seen much adoption of disk-to-disk-to-cloud backup yet?

I've seen a fair amount of adoption. People seem to be a lot more comfortable with disk-to-disk-to-cloud rather than directly going to the cloud or backup-as-a-service. Our most recent data found that 23% of companies said that they were using some form of disk-to-disk-to-cloud. And that's actually quite a bit. We also had a lot of people saying they were interested in it and investigating it. That's actually a lot further along than just pure backup-as-a-service or just disk to cloud.

The type of disk-to-disk-to-cloud backup companies are deploying depends on their size. Larger companies seem to be taking the model that I first described, which was to use their traditional on-premise backup and just replicate it to the cloud. Smaller companies tend to use the managed appliance from a supplier. But either way, the disk-to-disk-to-cloud is the much more dominant model in online backup.

A lot of people are familiar with disk-to-disk-to-tape. Why move from away from that approach for this hybrid cloud backup approach? What are the benefits?

There are a few reasons to use cloud over tape. The main benefit of going disk-to-disk-to-cloud is that you're automatically getting your data offsite. This is great for resiliency for disaster recovery and having your data go immediately off-site. On the other hand, if you went with disk-to-disk-to-tape, you'd have to take the tapes, encrypt them, and ship them off-site and deal with all of the physical movement.

One of the main reasons I see people considering a hybrid cloud backup service is because of the easy and quick digital transportation. There's also the fact that you don't have to handle the physical tapes. Getting tapes in and out of a library is time-consuming. Those are the main reasons that people tend to go that route, although there's definitely downsides to going with disk-to-disk-to-cloud rather than disk-to-disk-to-tape.

What are the drawbacks of disk-to-disk-to-cloud?

The first drawback is price. It's really hard to beat the price of tape. There's no storage medium that's cheaper than tape. We're seeing cloud storage get down there, but tape is still the cheapest. There are also all of the risks that you have with going with any service provider. That's not to say that it is extremely risky, but I find that a lot of people get nervous about putting their data in the cloud, and there's fair reason for that. There's the multitenancy aspect, and they're contracting with a third party, and so there's a lot of due diligence that has to be done around that. They must ask questions such as: What are their security models? How are they protecting your data? How are they storing your data? And are they using your data for something they shouldn't? So there's definitely an added risk in going to the cloud model, but on the other hand, there's the argument that you can lose tapes. You have to worry

about encrypting tapes. And sometimes you can lose tapes when moving them off-site. So I think there's definitely more of a perceived risk of going to the cloud, but I'm not necessarily sure that I believe that that is actually a true risk.

What vendors are currently offering disk-to-disk-to-cloud backup?

In the traditional on-premise backup provider space, the main vendors I see going disk-to-disk-to-cloud in enterprises are CommVault, EMC NetWorker, IBM TSM and Symantec NetBackup. These are really the main players, and there are a lot of them that can offer cloud as an eventual target for data. In the SMB and midmarket space, Acronis Inc., Asigra Inc., BakBone Software (recently acquired by Quest Software), EVault (a Seagate company) and Symantec with Backup Exec can also go to the cloud. So it's becoming a pretty common feature in on-premise backup solutions that they can use the cloud as a target. And it's not necessarily going to be any cloud—they usually have partnerships with different cloud providers that you can work with, or else maybe you can back up only to that company's proprietary cloud.

From the appliance perspective, providers that offer disk-to-disk-to-cloud offer it as a managed appliance that sits on-premise that you backup locally to and then replicate off-site. There are hundreds of vendors that provide this option, but the main player that I see in that space would be EVault, and Barracuda Networks (they acquired this technology through their acquisition of BitLeap a few years ago). These are the main players, but there are hundreds of them, and lots of resellers as well. ■

[Rachel Dines](#) is an analyst with Forrester Research.

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups

Blueprint for cloud-based disaster recovery

Cloud storage and computing services offer a number of alternatives for cloud-based DR depending on the recovery time and recovery point objectives a company requires. BY JACOB GSOEDL

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups

CLOUD COMPUTING, ALONG with mobile and tablet devices, accounts for much of the high-tech buzz these days. But when it comes to hype, the cloud seems to absorb more than its fair share, which has had the unintended consequence of sometimes overshadowing its real utility.

Although the concept—and some of the products and services—of cloud-based disaster recovery (DR) is still nascent, some companies, especially smaller organizations, are discovering and starting to leverage cloud services for DR. It can be an attractive alternative for companies that may be strapped for IT resources because the usage-based cost of cloud services is well-suited for DR where the secondary infrastructure is parked and idling most of the time. Having DR sites in the cloud reduces the need for data center space, IT infrastructure and IT resources, which leads to significant cost reductions, enabling smaller companies to deploy disaster recovery options that were previously only found in larger enterprises.

“Cloud-based DR moves the discussion from data center space and hardware to one about cloud capacity planning,” said Lauren Whitehouse, an independent storage consultant and analyst.

But cloud-based disaster recovery isn’t a perfect solution, and its shortcomings and challenges need to be clearly understood before a firm ventures into it. Security usually tops the list of concerns:

- Is data securely transferred and stored in the cloud?
- How are users authenticated?
- Are passwords the only option or does the cloud provider offer some type of two-factor authentication?
- Does the cloud provider meet regulatory requirements?

And because data is accessed via the Internet, bandwidth requirements also need to be clearly understood. There’s a risk of only planning for bandwidth requirements to move data into the cloud without sufficient analysis of how to make the data accessible when a disaster strikes:

- Do you have the bandwidth and network capacity to redirect all users to the cloud?
- If you plan to restore from the cloud to on-premises infrastructure, how long will that restore take?

“If you use cloud-based backups as part of your DR, you need to design your backup sets for recovery,” said Chander Kant, CEO and founder at Zmanda Inc., a provider of cloud backup services and an open-source backup app.

Reliability of the cloud provider, its availability and its ability to serve your users while a disaster is in progress are other key considerations. The choice of a cloud service provider or managed service provider (MSP) that can deliver service within the agreed terms is essential.

DEVisING A DISASTER RECOVERY BLUEPRINT

Just as with traditional DR, there isn't a single blueprint for cloud-based disaster recovery. Every company is unique in the applications it runs, and the relevance of the applications to its business and the industry it's in. Therefore, a cloud disaster recovery plan (aka cloud DR blueprint) is very specific and distinctive for each organization.

Triage is the overarching principle used to derive traditional as well as cloud-based DR plans. The process of devising a DR plan starts with identifying and prioritizing applications, services and data, and determining for each one the amount of downtime that's acceptable before there's a significant business impact. Priority and required recovery time objectives (RTOs) will then determine the disaster recovery approach.

Identifying critical resources and recovery methods is the most relevant aspect during this process, since you need to ensure that all critical apps and data are included in your blueprint. By the same token, to control costs and to ensure speedy and focused recovery when the plan needs to be executed, you want to make sure to leave out irrelevant applications and data. The more focused a DR plan is, the more likely you'll be able to test it periodically and execute it within the defined objectives.

With applications identified and prioritized, and RTOs defined, you can then determine the best and most cost-effective methods of achieving the RTOs, which needs to be done by application and service. In the rarest of cases, you'll have a single DR method for all your applications and data; more likely, you'll end up with several methods that protect clusters of applications and data with similar RTOs. "A combination of cost and recovery objectives drive different levels of disaster recovery," said Seth Goodling, virtualization practice manager at Acronis Inc.

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups

CLOUD-BASED DISASTER RECOVERY OPTIONS

Managed applications and managed DR. An increasingly popular option is to put both primary production and disaster recovery instances into the cloud and have both handled by an MSP. By doing this, you're reaping all the benefits of cloud computing, from usage-based cost to eliminating on-premises infrastructure. Instead of doing it yourself, you're deferring DR to the cloud or managed service provider. The choice of service provider and the process of negotiating appropriate service-level agreements (SLAs) are of utmost importance. By handing over control to the service provider, you need to be absolutely certain it's able to deliver uninterrupted service within the defined SLAs for both primary and DR instances. "The relevance of service-level agreements with a cloud provider cannot be overstated; with SLAs, you're negotiating access to your applications," said Greg Schulz, founder and senior analyst at Stillwater, Minn.-based StorageIO Group.

A pure cloud play is becoming increasingly popular for email and some other business applications, such as customer relationship management (CRM), where Salesforce.com has been a pioneer and is now leading the cloud-based CRM market.

Back up to and restore from the cloud. Applications and data remain on-premises in this approach, with data being backed up into the cloud and restored onto on-premises hardware when a disaster occurs. In other words, the backup in the cloud becomes a substitute for tape-based off-site backups.

When contemplating cloud-based backup and restore, it's crucial to clearly understand both the backup and the more problematic restore aspects. Backing up into the cloud is relatively straightforward, and backup application vendors have been extending their backup suites with options to directly back up to popular cloud service providers such as AT&T, Amazon, Microsoft Corp., Nirvanix Inc. and Rackspace. "Our cloud connector moves

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups

data deduped, compressed and encrypted into the cloud, and allows setting retention times of data in the cloud,” said David Ngo, director of engineering alliances at CommVault Systems Inc., who aptly summarized features you should look for in products that move data into the cloud. Likewise, cloud gateways such as the F5 ARX Cloud Extender, Nasuni Filer, Riverbed Whitewater and TwinStrata CloudArray, can be used to move data into the cloud. They straddle on-premises and cloud storage, and keep both on-premises data and data in the cloud in sync.

Cloud-based DR approaches side by side

	MANAGED PRIMARY AND DR INSTANCES	CLOUD-BASED BACKUP AND RESTORE	REPLICATION IN THE CLOUD
Instances	• Salesforce.com CRM • Email in the cloud	• On-premises into the cloud • Cloud to cloud	• On-premises into the cloud • Cloud to cloud
Merits	• Fully managed DR • 100% usage based • Least complex	• Only requires cloud storage; cloud virtual machines are optional • Usually less complex than replication	• Best recovery time objectives (RTOs) and recovery point objectives (RPOs) • More likely to support application-consistent recovery
Caution	Service-level agreements define access to production and DR instances	Less favorable RTOs and RPOs than replication	Higher degree of complexity
Implemented via...	N/A	Backup applications and appliances	• Replication software • Cloud gateways • Cloud storage software such as EMC Atmos and Hitachi HCP

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups

The challenging aspect of using cloud-based backups for disaster recovery is the recovery. With bandwidth limited and possibly terabytes of data to be recovered, getting data restored back on-premises within defined RTOs can be challenging. Some cloud backup service providers offer an option to restore data to disks, which are then sent to the customer for local on-premises recovery. Another option is a large on-premises cache of recent backups that can be used for local restores.

“I firmly believe that backups need to be local and from there sent into the cloud; in other words, the backup in the cloud becomes your secondary off-site backup,” said Jim Avazpour, president at OS33 Inc.’s infrastructure division.

On the other hand, depending on the data to be restored, features like compression and, more importantly, data dedupe can make restores from data in the cloud to on-premises infrastructure a viable option. A case in point is Michigan-based Rockford Construction Co., which uses a StorSimple appliance for cloud-based protection of its Exchange and SharePoint infrastructures. “In case of a disaster, we’ll pull VMs [virtual machines] from the cloud; with StorSimple’s deduplication we pretty much have to only pull down one full VM copy and the differences for others,” said Shaun Partridge, vice president (VP) of IT at Rockford Construction.

Back up to and restore to the cloud. In this approach, data isn’t restored back to on-premises infrastructure; instead, it’s restored to virtual machines in the cloud. This requires both cloud storage and cloud compute resources, such as Amazon’s Elastic Compute Cloud (EC2). The restore can be done when a disaster is declared or on a continuous basis (pre-staged). Pre-staging DR VMs and keeping them relatively up-to-date through scheduled restores is crucial in cases where aggressive RTOs need to be met. Some cloud service providers facilitate bringing up cloud vir-

tual machines as part of their DR offering. “Several cloud service providers use our products for secure deduped replication and to bring servers up virtually in the cloud,” said Chris Poelker, VP of enterprise solutions at FalconStor Software.

Replication to virtual machines in the cloud. For applications that require aggressive recovery time and recovery point objectives (RPOs), as well as application awareness, replication is the data movement option of choice. Replication to cloud virtual machines can be used to protect both cloud and on-premises production instances.

In other words, replication is suitable for both cloud-VM-to-cloud-VM and on-premises-to-cloud-VM data protection. Replication products are based on continuous data protection (CDP), such as CommVault Continuous Data Replicator, snapshots or object-based cloud storage such as EMC Atmos or the Hitachi Content Platform (HCP). “Cloud service provider Peak Web Hosting enables on-premises HCP instances to replicate to a Peak Web HCP instance instead of another on-premises HCP instance,” said Robert Primmer, senior technologist and senior director content services, Hitachi Data Systems.

NEW OPTIONS, OLD FUNDAMENTALS

The cloud greatly extends disaster recovery options, yields significant cost savings, and enables DR methods in small- and medium-sized businesses (SMBs) that were previously only possible in larger organizations. It does not, however, change the DR fundamentals of having to devise a solid disaster recovery plan, testing it periodically, and having users trained and prepared appropriately. ■

Jacob Gsoedl is a freelance writer and a corporate director for business systems.

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups

Cloud makes remote backups easier

Backing up remote offices and mobile devices has always been a challenge, but cloud backup services offer an easy, inexpensive way to protect branch office and mobile data. BY ALAN EARLS

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups

SOMEWHERE OUT THERE, far beyond the office tower or the headquarters building, important corporate data is sitting on a desktop, laptop, or server waiting to be backed up. It can be a long wait. “Remote backup” is almost always a byword for low-priority, second-string technology and trouble waiting to happen.

However, the good news is that there are more options than ever for keeping data at remote office and branch offices (ROBOs) safe—perhaps even just as safe as the data at headquarters. While tape seems to be falling from favor for remote data backup, or ROBO backup, a wide range of new solutions are emerging—including cloud-based backup and other disk-based approaches.

Take the example of Medical Management Innovations Inc. (MMI), a company that has tried both approaches for remote office backup. Specializing in providing medical field case management services, MMI’s “bread-and-butter” is handling confidential and HIPAA-protected medical information, which a large force of remote workers handle on their laptops.

GETTING THE BEST OF BOTH WORLDS WITH REMOTE BACKUPS

Rich Pflederer, company president, had been subscribing to Mozy, a remote cloud-based backup service. However, he noted, as the company continued to expand, the backup costs kept going up in direct proportion to the number of devices in use, with no end in sight. With more than half the staff working from home on laptops, his priorities included ease of use and controlling or reducing monthly fees. “I wanted something that would provide the best of both worlds, where we could own it,” he said. After doing some shopping, Pflederer purchased a Remote Backup Appliance from 3X that offers cloud and local capabilities. Data is backed up to a remote location and locally on the appliance. “Now, when we need it, we can physically do a restore right in our office,” he said.

Dave Cowlin, president, H.L. Hamilton Insurance, in Amherstburg, Ontario, Canada, has faced similar challenges. His company has eight employees divided between two locations. One site did tape backup, once a day, and the other did backup to an external hard drive. In both cases, the “system” relied on employees swapping media and taking media home “for safe keeping.”

Although the system worked, Cowlin said it “wasn’t the smartest way to handle important information.” About two years ago, Cowlin said he started searching out alternate data backup solutions that didn’t depend so much on the reliability of employees. After looking at the available options proposed by a third-party solutions provider, he settled on ROBObak network-based data protection software—a private cloud approach to backup coupled

About two years ago, Cowlin said he started searching out alternate data backup solutions that didn't depend so much on the reliability of employees.

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups

with deduplication that also provides the option of local backup when needed. (RoboBak is now part of KineticD.) “It was relatively hands-off, pretty simple to use and it was competitive cost-wise,” he said. “Now, ROBObak is scheduled so it initiates backups automatically and sends a report via email when it is done. That way I have a verification that it was completed,” added Cowlin. He said he is also considering having remote backup data automatically copied to “opposite” offices to provide increased data protection.

CLOUD-BASED BACKUP AND OTHER COST-EFFECTIVE APPROACHES

Lauren Whitehouse, an independent storage and data protection analyst, said the problem with remote offices is that companies frequently don’t have any local IT capability to manage the kind of remote office backup solution that might be ideal. “Things like tape-based backup can be automated to some extent, but eventually someone has to change a tape and if you have a drive error, you really need to have someone look at it,” she noted. That presents a resource issue for a lot of organizations, which explains why many companies are shunning the tradition of local tape backup in favor of alternatives like data deduplication coupled with disk backup as well as various forms of cloud-based backup.

Whitehouse said many organizations have moved away from tape at their remote offices and have implemented disk-based deduplication so they can keep data for longer period and have the added benefit of consolidating backups from different locations to a central point. This scenario—like the ROBObak example—can still allow for local recovery.

Whitehouse said all the major backup products can be stretched to manage remote backups, with the advantage of “having one policy engine” for the whole organization. However, Whitehouse said many organizations end up running multiple backup apps

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups

to meet the specific needs of their remote and central facilities. Among the fastest growing remote backup solutions are appliances such as those offered by Unitrends and SonicWALL (now part of Dell), which offer on-site backup as well as the option of transferring remote backup data back to a central location, “So you don’t have to deal with having backup software and finding the right disk target.” But they are not without problems. In other words, they simplify things in one sense but often introduce a new layer of management because “now you might be managing one solution for a central corporate location and other solutions out at the edge,” she noted. “If you have multiple locations, each with a different solution, that can become very complex.

Are some [remote backup] solutions better for large and small companies? Whitehouse said, “It depends on your bandwidth.”

DIFFERENT ROBO BACKUP OPTIONS FOR DIFFERENT COMPANY SIZES

Are some [remote backup] solutions better for large and small companies? Whitehouse said, “It depends on your bandwidth.” Trying to “drag” large quantities of data across a WAN can consume resources. However, she noted, “even if you look at some of the solutions that dedupe at the source, like Avamar, [Symantec NetBackup] PureDisk and CommVault, you can still have similar issues. Some organizations will simply load up a portable device with the data and ship it; then they can just trickle additional changes over subsequently, she noted. The same challenges can apply with cloud vendors—doubly so because recovery activities run into bandwidth challenges, too.

Certainly, said Whitehouse, cloud-based backup is a viable option, either by means of a private cloud—which still really means

backing up to headquarters—or through a service offering. “There are also some hybrid applications that allow for a local copy, too,” she added. Examples of “hybrid” backup SaaS solutions include: Ax-cient Inc., EVault (a Seagate company), IBM Corp., SunGard, Vault-Logix, Venyu Corp., as well as Asigra- and Nine Technology-based products (both of these vendors license to managed service providers who typically re-brand the service).

Whitehouse said these products offer both local disk and cloud storage. The more sophisticated offerings allow subscribers to specify the capacity of backup data that resides in each location.

“This is important to manage backup retention on- and off-premises. Without that level of flexibility, the solution may get expensive or not meet retention objectives,” she said. For example, users may want to only hold two to four weeks of backup data locally and keep the rest in cloud-based storage for longer-term retention

(months to years). “With a one-to-one alignment of on- and off-site data, an organization would have to either hold months to years on on-site disk or be limited to weeks to months of off-site cloud storage,” she said.

Rachel Dines, an analyst at Forrester Research, said regardless of the specific solution, companies are doing more to consolidate remote backups and simplify operations. “The most common solution I am seeing emerge is backing up to a small deduplication appliance and replicating back to the main data center, she added. There are many examples of such systems, EMC Data Domain being one of the best known. “The major vendors often have similar products for large data centers and have developed devices suitable for local use,” said Dines.

More sophisticated offerings allow subscribers to specify the capacity of backup data that resides in each location.

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups

Dines said if you backup that way, the replication cost is low because you are replicating deduped data and if you need to do a restore, you can retain a copy of the backup. The downside, of course, is that you need to invest in the appliances. “They aren’t cheap, and if you have a lot of small offices, it might simply be too expensive,” she added.

Other options are source-based deduplication products, which can make backups for smaller offices more feasible at a lower price. Products that fit this description include CommVault Simpana, EMC Avamar, IBM’s TSM and Symantec Corp. NetBackup. However, she noted, this solution style “won’t really work well for anything more than a few hundred gigs.”

Going straight to the cloud can also work. But many organizations prefer an intermediate step. “I am seeing a fair number of companies with on-premises backup in the data center but in remote backup they are doing disk-to-disk-to-cloud or disk-to-cloud. So they don’t have to worry about pulling data back to the site. And there are many vendors providing cloud-based backup-as-a-service. “The ones doing a lot of branch office support are EVault and various smaller service providers using OEM solutions from Asigra and Geminare,” she said.

“None of these paths are mutually exclusive—you could supply any combination of those technologies to achieve your backup goals,” she said. But clearly local tape backup is dying. “Having a tape appliance at every branch is costly and time-consuming.” However, she added, the exception may be smallest companies, where tape still has a relatively secure niche because it is well-established and inexpensive. ■

Alan Earls is a freelance writer.



TechTarget Storage Media Group

Storage magazine

Vice President of Editorial
Mark Schlack

Editorial Director
Rich Castagna

Senior Managing Editor
Kim Hefner

Executive Editor
Ellen O'Brien

Contributing Editors
James Damoulakis,
Steve Duplessie, Jacob Gsoedl

SearchStorage.com

Executive Editor
Ellen O'Brien

Senior News Director
Dave Raffo

Senior News Writer
Sonia R. Lelii

Senior Writer
Carol Sliwa

Senior Managing Editor
Kim Hefner

Assistant Site Editor
Ian Crowley

SearchCloudStorage.com

Executive Editor
Ellen O'Brien

Assistant Site Editor
Rachel Kossman

[SearchDataBackup.com](#)
[SearchDisasterRecovery.com](#)
[SearchSMBStorage.com](#)
[SearchSolidStateStorage.com](#)

Senior Site Editor
Andrew Burton

Managing Editor
Ed Hannan

Assistant Site Editor
John Hilliard

Features Writer
Todd Erickson

[SearchVirtualStorage.com](#)
[SearchStorageChannel.com](#)

Senior Site Editor
Sue Troy

Assistant Site Editor
Francesca Sales

SearchStorage.co.UK

Senior Site Editor
Sue Troy

UK Bureau Chief
Antony Adshead

Assistant Site Editor
Francesca Sales

Storage Decisions

TechTarget Conferences

Director of Editorial Events
Lindsay Jeanloz

Editorial Events Manager
Jacquelyn Hinds

Storage magazine subscriptions:

www.SearchStorage.com

Storage magazine
275 Grove Street
Newton, MA 02466

editor@storagemagazine.com

TechTarget Inc.
275 Grove Street, Newton, MA 02466
www.techtarget.com

©2012 TechTarget Inc. No part of this publication may be transmitted or reproduced in any form or by any means without written permission from the publisher. TechTarget reprints are available through The YGS Group.

About TechTarget: TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.

Cloud backup
benefits

Enterprise
cloud backup

Hybrid
cloud backup

Cloud-based
DR blueprint

Remote
cloud backups