

## WHITE PAPER

---

# Key Criteria in Selecting a Cloud Backup Provider Built to Last

Sponsored by: EMC Mozy

---

Liz Conner

Laura DuBois

May 2013

## IN THIS WHITE PAPER

Cloud services are having a transformational effect on IT organizations today. They are changing not only how IT is architected, procured, and deployed but also from whom and how IT infrastructure is provided. Storage is one industry seeing major disruption as consumers and businesses alike procure storage capacity and functions from public cloud service providers. However, paramount to a sustainable and successful deployment of a public cloud storage service is extensive due diligence on the cloud provider offering the service. This paper identifies the key criteria that firms should use in evaluating a cloud service provider business that is built to last. It also identifies how Mozy by EMC Corporation addresses these requirements, empowering over 100,000 business customers and millions of individuals to rely on the Mozy cloud for protection and recovery of their data.

## SITUATION OVERVIEW

---

### The Growth of Cloud and Its Impact

Cloud services, along with mobility, big data/analytics, and social media, are one of the four leading transformational technologies enabling new business and IT strategies. Cloud services have changed the manner in which some applications are developed and how major portions of IT infrastructure are purchased, managed, and deployed. They allow companies to outsource select portions of their compute, storage, and/or data needs, resulting in capital and operating cost savings for strained IT budgets. Cloud services allow organizations to purchase just what they need while benefiting from more easily upgraded services and eliminating the need to overprovision hardware in anticipation of future growth. The maintenance of IT infrastructure cannot be overlooked either. The ongoing monitoring, troubleshooting, and management of infrastructure and applications can be offloaded from internal operations teams to a cloud provider.

As cloud computing continues to grow, the storage component is leading the way. Consistently, going back to 2006 when IDC first initiated its cloud research, storage has been one of the leading use cases for public cloud. According to IDC's 2012 *CloudTrack Survey* of 493 IT professionals, behind email, backup/archive was the number 2 workload most likely to migrate to the public cloud. Why is this? For organizations seeking quick deployment of increased storage or enhanced desktop/laptop backup, within the limits of established operating budgets (opex), public cloud storage services offer relatively hassle-free, off-premise, pay-as-you-grow storage. The leading use cases for these types of

deployments on both public and hybrid clouds are backup, storage, and disaster recovery. By backing up to the cloud, organizations averse to capex approaches can save money by not having to build or manage a physical backup site with physical storage and also have a built-in disaster recovery solution in case something happens to their primary on-premise datacenter facility.

While the majority of IT organizations continue to prefer trusted on-premise storage approaches — NAS, SAN, and so forth — for critical needs such as storage for virtual machines, database, and transactional applications, IDC believes that backup and disaster recovery will continue to be key factors in cloud computing growth. Among 163 IT and storage professionals surveyed in IDC's March 2012 *Disk-Based Data-Protection Survey*, approximately 64.5% of firms are using or planning to use a public cloud backup strategy. This same survey highlights that of the 38% that are currently using the public cloud for backup, it is for a relatively small but growing percentage of their overall data volume.

However, as cloud computing, and with it cloud backup, becomes more popular, we start to see distinctions between various types of cloud backup services and providers, as vendors carve out new target markets and different groups require cloud backup with different attributes.

☒ **Consumer versus enterprise:** There are obvious distinctions between the needs of consumers and enterprises, which can be seen in the storage capacity needed, application support required, need for administrative tools and functionality, bandwidth availability to meet data volume, number of users, security features required, customer support, uptime, and payment models (freemium versus paid subscription). Although consumer requirements should not be taken lightly, enterprise customers need a provider that is adept at handling specific enterprise needs. Specific enterprise needs typically span requirements around data security, privacy and location, application/client support, effective handling of large data volumes, and supporting services that can run over shared or private, point-to-point networks.

☒ **Start-up versus established provider:** Cloud services represent growth for the IT industry and offer relatively low barriers to entry for innovative new companies. As a result, small start-ups are targeting and will continue to target niche markets that are currently being underserved or attempt to provide a distinct/new service, pricing model, features, and so forth. To minimize start-up costs, many leverage third-party infrastructure as a service (IaaS) rather than stand up their own hardware. Thus a cloud service may be dependent on a third party to meet SLAs, and troubleshooting can be complex. Conversely, established cloud providers tend to build and operate their own clouds, targeting either the consumer population or the general business/enterprise world or, in some cases, both. Established cloud providers have gone through successful certification and audit processes as well as have valuable experience in deploying and managing cloud infrastructure. The established provider may also offer richer SLAs, more customized offerings, and the business and financial viability absent in start-up offerings.

Public cloud backup has become an increasing integral part of corporate IT. Many different factors go into distinguishing what different providers can offer. According to IDC's storage in the cloud forecast, IDC estimates the public cloud backup services

market will reach over \$2 billion in spending in 2013 and see a 33% compound annual growth rate (CAGR) from 2010 to 2015, reaching over \$3.6 billion in spending by 2015. With material spending on public cloud services for backup dramatically outweighing the more modest 4.8% CAGR for the traditional on-premise data backup software market, choosing the right service provider has never been more important, especially with a function like backup that is notoriously long lived in terms of data, format, and footprint.

## **CRITERIA IN CHOOSING A CLOUD BACKUP PROVIDER**

For enterprise organizations to determine which cloud backup provider is most suited to their needs, it is important to establish certain criteria that must be met by a potential provider. The following criteria are the leading features that should be evaluated when choosing a cloud backup provider. These criteria can be used by firms in conducting their due diligence on service providers, offerings, and contractual agreements.

---

### **Service Provider Business That Is Built to Last**

Given the nature of cloud backup, a cloud backup provider must be in it for the long haul. Although start-ups and even established players might present initial cost savings or unique features, if they are going to be out of business in the next five years, they pose a huge liability to their potential clients. When a firm leverages on-premise server or storage hardware, if the IT supplier goes out of business, clients no longer have a company to call for maintenance/service and must eventually move their applications or stored data to a different system. However, this transition can usually be done as needed and, if migration is done successfully, without any data loss associated with the exit of a storage hardware company. The same cannot be said for a cloud provider. When cloud providers exit the market, there is risk that they have done so with their customers' data, resulting in potential security concerns, data loss, and corporate stakeholder visibility. To ensure that a cloud backup provider is built to last, potential clients should examine the following categories closely.

**Financial stability:** If the cloud provider is not in a profitable financial position or is still trying to establish a successful business model and/or customer base, there is a high degree of risk that this will be a losing venture and the company will fold. Questions to ask to verify a service provider's financial stability include (responses may be disclosed under a signed NDA):

- Are you profitable today? If not, when do you forecast your breakeven?
- What is your cash position?
- What is your current credit rating?
- Can you please provide a signed copy of your company's most recent audited financial statements?
- Has your company filed for bankruptcy protection? When? Why?

**Proven infrastructure:** Although innovative technology and hardware can help streamline an industry or establish new industries, in the case of cloud backup, the infrastructure being implemented by the cloud provider must be a proven one for an enterprise customer to entrust the cloud provider with critical corporate data. As mentioned previously, many cloud backup services may rely on third-party IaaS and are thus in a dependent relationship to satisfy SLAs or troubleshoot issues. Questions to ask to establish if the service provider is leveraging a proven infrastructure include:

- Do you operate on a buy-and-operate model, or do you rely on IaaS providers?
- In either scenario, what are the SLAs for service uptime, resiliency, backup success, backup times, restore times, etc.?
- Are SLAs documented and published?
- For service providers that leverage commercial hardware and software rather than build the infrastructure themselves, what hardware and software infrastructure is used?
- How long has this infrastructure been in production?

**Established customer base:** When looking for a provider, it helps to know which other businesses are currently using the provider's services. A small customer base, although growing, would indicate more of a start-up. Loss in customer base would indicate something is wrong and making clients leave. Ensure that service providers that quote thousands or millions of customers are referencing business customers, not just consumers. Many service providers start with a consumer or SMB focus but may not yet be established enterprise providers. To minimize risk, look for a provider with a large enterprise clientele. Use your internal or peer network to speak with customers of a given service provider. Questions to ask include:

- How many consumers use your service today? Are these freemium or paying customers?
- How many businesses use your service today? Are they SMB or enterprise customers?
- What is the growth in each segment you have seen in the past 12 months or 24 months?
- How long have you been serving enterprise customers?
- Are there customers that are not suited for your service? Which ones? Why?

**Geographically distributed datacenters:** As Hurricane Sandy in 2012 showed some, it is helpful if the cloud datacenter that holds the backup files is not located 25 miles down the coast (when a natural disaster hits). Geographically distributed datacenters become important to ensure that there are failovers if constant uptime is mandated and there is an unforeseen problem with the primary datacenter where data is located. Location is important in order to diversify risk, especially in the case of natural disasters but also to comply with regional jurisdictional requirements for data location. For example, some geographies have requirements that data not leave regional borders, which necessitates a service provider have physical facilities in that region. Questions to ask include:

- Are your datacenters geographically distributed, and do you have datacenters outside of the United States for customers located in Europe or Asia/Pacific, for example?
- Can you ensure my data will go to a given datacenter?
- What is your business continuity plan in the event of site or operational failure?

**Third-party validation and accreditation:** Periodic, successful audits of a cloud backup provider's security procedures are essential to verify the cloud provider's processing and hosting of customer data is done safely and securely. SSAE 16 is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA) that verifies whether a service organization has been through an in-depth audit of its control objectives and control activities to ensure safe and secure process and hosting of customer data. Additionally, ISO 27001 certification establishes a potential cloud provider as having met international standards for measuring information security management systems. ISO 27001 is a set of requirements and best practices for a systematic approach to managing company/customer information based on periodic risk assessments appropriate to ever-changing threat scenarios. Consider if your service provider has answers to the following:

- Have you been through any third-party security audits in the past 24 months? By whom and when?
- Please provide the results of those audits.
- Does your business have ISO 27001 or ISO 27002, SSAE 16, PCI DSS, HIPAA, or other certifications?

**SLA terms and execution:** Established SLA terms and execution are integral not only to establishing how a customer's data will be processed and hosted but also to setting a transparent level of service the customer can expect from the cloud provider. This helps set expectation levels and establish the anticipated level of service. Questions to ask your service provider include:

- How are SLAs monitored and measured and by whom?
- Are there any business disruptions these SLAs would not cover? Please describe.

## Service Built on Leading Security and Privacy Practices

One of the major concerns of cloud backup is the security and privacy of the data. Companies are concerned with illegal outside intrusion to their data (aka hacking), potential seizure of cloud provider hardware by government authorities, and cloud providers using unauthorized access to the data to mine statistics or sell data. Given that the backup data is physically not in the control of the enterprise, security and privacy concerns will always be at the forefront of the enterprise IT department. Therefore, it is paramount that a cloud provider offer the utmost in security and privacy features. Essential security features for an enterprise customer include:

- Personal key AES encryption:** The ability for the customers to set up and maintain their own personal encryption keys, which they — not the service provider — control. AES is considered the standard for encryption, being used by various government agencies and being FIPS certified. More importantly, the ability for the customers to set and manage their own encryption keys means the cloud backup providers cannot decrypt their files, even under force of law.
  - Does your organization have a formal, documented, mandated, companywide information security program, including security policies, standards, and procedures? Please provide.
  - Do you require data to be encrypted during backups? What level of encryption?
- Encryption over the wire and at rest:** Ensuring the data is encrypted while it is transferred to cloud backup providers (over the wire) and while it is stored within cloud backup providers' systems (at rest). The combined use of these two encryption types helps establish stronger data security than if only one was used. Of course, encryption must be done in effective concert with storage efficiency strategies such as compression and deduplication.
- Key management/handling:** Establishing who has control over the encryption key, whether the key management/knowledge resides with the cloud backup provider or whether the customer maintains all management and knowledge of the encryption key. If key management resides with the customer, the cloud backup provider must have a process in place to ensure that the encryption key is stored locally with the customer and not on the cloud provider's system. Varying levels of key management are desirable to meet various customers' needs.
  - Ask service providers to describe their organizations' encryption key handling infrastructure.
  - Ask service providers to describe their organizations' options for handling encryption keys.

**Documented, mandated, and monitored security program:** Make sure that the cloud provider has a security program in place and that it is well documented and meets all mandates. This will help establish the security credibility of the cloud provider.

- Are security policies documented?
- Does the service provider have a dedicated security organization?
- Have they undergone a vulnerability assessment by a recognized third party? Can you provide results?

In terms of privacy concerns, the following are key privacy features enterprises should look for in a potential cloud backup provider:

**Documented, mandated, and monitored data privacy policies:** Enterprise clients want to make sure that cloud backup providers have policies in place to address any and all privacy concerns. This will help establish the credibility of cloud providers as they have taken the time to establish and document privacy policies. Questions to ask a cloud provider include:

- Do you have a privacy policy published and accessible to personnel? Is it reviewed and approved by a board-level committee?
- Will you permit an independent company to verify your privacy procedures?

**Policy on user advertising/data mining:** Cloud providers must be transparent with their policy on the use of client data — whether the cloud provider will have access to it for advertising and/or data mining purposes or whether the access to the data is strictly prohibited to all except for the client. Enterprises' feelings regarding advertising/data mining use will vary, but cloud backup providers must be up front and transparent in their policies regarding their use of client data.

- Please explain your policies on use of customer data for advertising or mining this data for monetary gains.

**Practices for safeguarding confidential or sensitive information:** Certain data, more so than all data, is of the confidential or sensitive type. This type of data requires additional privacy protocols. Cloud providers must have an established practice for additional safeguards regarding sensitive material.

- Do you have procedures implemented to ensure personnel and contractors maintain the security and confidentiality of your data? Please describe.

## Service Enabling Leading Data Management Processes

In addition to security and privacy concerns, another characteristic that should be of note is a service that is built with world-class data management. Features of successful data management include but are not limited to the following:

- ☒ **Centralized management framework.** Administrators or nontechnical personnel should be able to centrally manage, report on, and monitor a cloud service that is being performed by a service provider. This should include the ability to push out reports as well.
- ☒ **Providing support for a range of clients and applications.** Often customers start with a discrete application or set of clients and then expand to protect other systems. Rather than invest in different cloud services for each asset type, the ability for one cloud service to protect and recover a range of data from a range of systems is an imperative.
- ☒ **Active Directory (AD) or LDAP integration.** Support for AD or LDAP is essential in making an enterprise-scale deployment as easy as possible. Integration with user and group accounts makes adding or removing users from a cloud service relatively seamless.
- ☒ **Enabling a range of services.** While customers often start with backup, they soon realize they face other requirements too. Users may be asking for functions such as file synchronization and recovery. The ability for a single service deployment (and agent) to support a range of functions offers operating and capital savings.
- ☒ **Data seeding.** Seeding of a customer's first backup by prepopulating a storage system that is shipped to the cloud provider is integral in reducing bandwidth usage and time/cost of standing up the initial backup.
- ☒ **Hybrid cloud.** Presenting the option of having a local backup in addition to a cloud backup for mission-critical data will help cloud providers ensure the fastest time to recovery for essential data.

## WHY ENTERPRISES CHOOSE MOZY CLOUD BACKUP

As enterprises evaluate potential cloud backup providers, Mozy leads the short list of preferred providers. Founded in 2005, Mozy is a proven leader in the cloud backup space and is backed by storage leader EMC. Mozy caters to a wide range of clients, including individual consumers as well as Fortune 100 enterprises, and provides a number of services tailored to its broad customer base. For the enterprise customer, Mozy offers easy-to-manage cloud backup, the ability to scale across multiuser environments, numerous security features including AES key management choices, and enterprise storage software features such as snapshots to ensure comprehensive data retention.

To focus on enterprise customers' cloud backup needs, Mozy has specifically looked to address the key features most important to enterprise customers.



Mozy offers a number of key features to the cloud backup market (see Table 1). These key features help Mozy differentiate itself from competitors in the market.

**TABLE 1**

Checklist of Key Cloud Backup Features

	<b>Mozy's Features</b>
<b>Built to last</b>	
Financial stability	Mozy is a cloud service offered by EMC, a \$47 billion publicly traded company.
Proven infrastructure	The Mozy cloud services have been running in production for over eight years. The hardened backup infrastructure includes 90PB of cloud data under management.
Established customer base	Mozy has over 100,000 business customers and over 6 million end users of its services. Mozy has been providing cloud backup services to enterprise customers since 2008.
Geographically distributed datacenter locations	Mozy has a network of geographically distributed datacenters including datacenters in the Americas and EMEA for customers and partners in those geographies.
Certifications	Mozy is ISO 27001 certified and Safe Harbor compliant.
Successful audits	Mozy has successfully completed a SSAE 16 Type II audit.
SLA terms and execution	Mozy manages to three-nines service availability.
<b>Security</b>	
Private key AES encryption	Mozy offers private AES encryption with its personal key and enterprise customer key.
Encryption over the wire and at rest	All data is encrypted during the backup process, sent over an encrypted SSL connection, and encrypted while at rest for complete end-to-end data protection.
Key management/handling	Mozy offers three levels of key management: a default key, using Blowfish and managed by Mozy; a personal key, using AES and managed by the individual; and an enterprise custom key, using AES and managed by the enterprise customer.
Personnel security	Mozy has a personal security program in place that includes background checks, access management, and auditing.
Documented, mandated, and monitored security program	Mozy has an ISO Information Security Management System in place.
Security policies	Mozy has a dedicated cloud security team that develops and maintains comprehensive physical and digital security policies. Mozy's security policies may be shared with customers on an as-needed basis.
Penetration testing and vulnerability assessments	Vulnerability assessment is performed quarterly or as needed. Penetration testing is performed by the Mozy security team as needed in support of the vulnerability assessment program.

**TABLE 1**

## Checklist of Key Cloud Backup Features

	<b>Mozy's Features</b>
<b>Privacy</b>	
Documented, mandated, and monitored data privacy policies	Mozy's privacy policy is documented on its Web site (available at <a href="http://mozy.com/privacy">mozy.com/privacy</a> ).
Policy on user advertising/agreement not to mine customer data for advertising	Mozy does not sell or market user data and does not view end-user backup data.
Practices for safeguarding confidential or sensitive information	Mozy has both data classification and handling policies, along with information handling procedures, which define various levels of data classification and the controls associated with those levels.
Compliance with regional or local data privacy regulations	Mozy is Safe Harbor compliant and offers a network of geographically distributed datacenters.
<b>A service built with world-class data management</b>	
Centralized management	Mozy offers a Web-based, multitenant admin console for account management by administrative and sub-administrative personnel. The Mozy software may be configured, deployed, and centrally managed via the admin console, which offers comprehensive custom configuration controls.
Range of clients and applications supported	Mozy supports a range of applications, including network shares, all versions of SQL and Exchange, SharePoint, Active Directory, COM+ services, SYSVOL directory share, and Windows Registry databases.
Active Directory integration	Mozy offers Active Directory integration that automatically triggers user creation, organization, and removal in MozyEnterprise.
Range of services	Mozy offers consumer-based cloud backup, business cloud backup (both end user and server), and enterprise cloud backup.
Policies for backup and retention	MozyEnterprise offers a 90-day retention policy.
Seeding: First backup	Mozy offers Mozy Data Shuttle, a device to seed the initial backup into the Mozy cloud.
Hybrid option for local recovery and fastest time to recovery	Mozy 2xProtect allows for a local backup to be made to a USB or an external drive in addition to the cloud backup. Additionally, complementary BRS on-premise backup solutions are optimized for hybrid cloud backup.

Source: IDC, 2013

## **CHALLENGES/OPPORTUNITIES**

Over the years, Mozy has established itself as a leading cloud backup provider with consumer and enterprise customers. Mozy has been diligent in addressing the key concerns all customers have regarding public cloud, data privacy, and security. Introducing features such as AES encryption, private key management, access and logging, audit trails, ISO 27001 certification, SSAE 16 auditing, and numerous datacenter locations has helped Mozy establish a strong reputation among cloud providers.

The next layer of distinction will come with refining how data is efficiently moved, stored, and recovered. Addressing the size of a data volume versus the data pipe used to move it will highlight the need for storage efficiency technologies. Another challenge is revealed in different workloads potentially requiring different recovery options to most efficiently recover the data. A range of options would need to be implemented in order to address this. By addressing these concerns, Mozy has the opportunity to provide value-added services few are focusing on and once again show why it is a leader in cloud backup.

## **CONCLUSION**

As enterprise organizations streamline their datacenters in the most cost-efficient and effective manner possible, an opportunity continues to evolve for cloud backup services. To reduce datacenter costs — especially storage hardware, building footprint, and power and cooling costs — enterprises are looking to public cloud providers for offsite data backup and disaster recovery services. As enterprise interest in cloud backup grows, so does the need for a competent cloud provider. Improved focus on enterprise-specific needs, such as extensive privacy and security features, easy account management and multiuser administration, 24 x 7 support, and scalability, establishes Mozy as an industry-leading cloud backup provider that should be on an enterprise's cloud provider short list.

---

### **Copyright Notice**

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2013 IDC. Reproduction without written permission is completely forbidden.