IDC
Analyze the Future

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

WHITE PAPER

The Benefits of Cloud-Based Backup: Addressing Business Continuity in a Distributed Workforce

Sponsored by: Mozy

Brad Nisbet Laura DuBois

September 2011

EXECUTIVE SUMMARY

Firms of all sizes among many different industries struggle with how to store, protect, and manage growing amounts of business information. Increasingly, business-critical data extends beyond a centralized location within the organization and spans a distributed, often mobile workforce. For many small and medium-sized businesses (SMBs) and smaller branch offices of larger organizations, it is imperative to protect data among this distributed set of assets and provide the means for business continuity in the case of data loss.

The reliance on business data and the need to protect that data are pervasive and intensifying. A wide variety of business types are seeking effective methods to protect critical business information. Just about any business — including accountants, florists, and doctors — is exposed if it does not have a secure data protection plan in place.

Often, the ability to address these business continuity concerns is limited due to minimal staffing resources and restricted budgets. In addition, traditional solutions that address data protection and data sharing across a variety of centralized storage and mobile devices can be elusive. With the advent of cloud-based storage approaches, new options have emerged to address the concerns many organizations have regarding data protection, business continuity, costs, and manageability.

SITUATION OVERVIEW

Data Challenges in Today's SMBs

Today's SMBs and branch offices face many challenges associated with storing, protecting, and managing increasing amounts of business data. As organizations move to more comprehensive plans to protect their data and provide business continuity, they are often responding to the following pain points:

- **A distributed workforce and diverse assets.** A growing base of mobile users with an ever-expanding spectrum of devices to access, store, and share data has created more complex data storage environments. According to IDC's *Worldwide Mobile Worker Population 2009–2013 Forecast*, the world has over 1 billion mobile workers (those who are not tethered to a desktop, who use laptops and/or other mobile computing devices). The United States has almost 120 million mobile workers (almost 75% of the workforce). With a growing distributed

workforce, the complexities range from protecting data across the diverse environment to the ability to collaborate and share business information among myriad users.

- **Capital costs.** Maintaining the appropriate levels of storage capacity can be costly. Backup in particular can be a costly proposition for any firm and one that provides no real incremental value to an organization. The growth in data volumes, which is averaging 52% annually, has a downstream effect on backup. Technologies such as deduplication can help curb growth, but, ultimately, more data needs to be protected. This growth requires investment in additional backup infrastructure, including media, software licenses, tape drives, and media servers.

- **Operational costs.** The nature of backups in most firms today means a never-ending process of checking for backup successes, troubleshooting failures, planning for capacity upgrades, dealing with performance bottlenecks, and initiating user restores. These routine backup processes require human resources and divert technical talent from more strategic IT projects.

- **Management of removable media.** Most disaster recovery programs include a best practice where data is moved offsite, typically while resident on removable media such as tape. This introduces several challenges, including physical longevity of the media, security risks, tape collection costs, and labor in tracking tape media for rotation. Tape budgets need to be updated if data is retained on tape for long periods of time.

- **Data growth.** Organizations are generating unprecedented amounts of data, and SMBs are struggling to simply keep up with data storage requirements. Growing data volumes place increasing pressure on constrained backup windows.

- **Lengthening retention periods.** As organizations look to leverage the value of their business information and address compliance or regulatory concerns, they are required to store the data for longer periods of time. Compounding this issue is the ability to gracefully and efficiently retrieve subsets of data among a vast amount when and where needed. Organizations seek to address long-term retention with backup solutions, thus increasing requirements for backup processes.

- **Disaster recovery.** Recovery times are compressing as business reliance on IT continues to grow. For many SMBs and branch offices, disaster recovery is often overlooked or is inefficient and ineffective because self-management of offsite data copies can be challenging and costly and may introduce security risk.

The challenges of storing, protecting, and sharing expanding volumes of business data can leave SMBs and branch offices overwhelmed and looking for alternatives to help reduce strain on resources and provide lower-cost solutions. In particular, organizations are looking for the ability to provide a comprehensive data backup solution that spans both centralized data (on servers) and distributed data (on laptops, PCs, and other mobile devices). With the advent of cloud-based storage solutions, especially those that are addressing concerns around backup and recovery within a distributed environment, SMBs and branch offices have a sound, new alternative to consider.

Cloud-Based Backup: An Attractive Alternative to an On-Premises Approach

Cloud-based backup is a service by which business information is backed up over the Internet to a shared storage infrastructure at an offsite datacenter location, maintained by a third party. In this scenario, a backup agent is typically deployed on on-premises servers that hold data to be backed up. Data associated with on-premises systems are backed up to hosts in the cloud.

Among cloud-based storage services, backup is the largest and most popular segment of advanced services, which comprise backup, archiving, and business continuity (replication). IDC estimates that the worldwide market opportunity for cloud-based backup was $942 million in 2010 and forecasts that it will grow at a compound annual growth rate of 28% to $2.5 billion in 2014.

Benefits of Cloud-Based Backup

Cloud-based backup allows the SMB or branch office to establish an effective process for comprehensive data protection and business continuity in the case of data loss. In addition, the cloud-based approach transfers nearly all of the concerns and challenges associated with deploying and managing a growing backup environment to a third-party provider. In particular, cloud-based backup provides the following benefits:

- **Comprehensive business continuity and accessibility.** Establishing a common repository of data that is used by the entire organization leads to comprehensive business continuity and protection against data loss across the organization. In addition, data can be shared among a larger community of users. This is especially true for larger businesses or multiple branch offices working together over geographically dispersed environments. Backup solutions that span multiple types of devices (from servers to PCs to mobile devices) will serve the organization well to provide business continuity and reduce backup and data sharing complexities among such a diverse environment.

- **Lower capital cost.** Depending on the level of adoption, a cloud-based backup service allows the customer to reduce, if not eliminate, the need for capital on storage capacity (disk, tape, and/or other removable media) associated with backup processes. With a subscription-based pricing model typically employed by cloud-based backup providers, the cost associated with backup becomes a more predictable operational expenditure.

- **Reduced strain.** The limited IT staff is no longer overwhelmed because cloud-based backup can reduce or eliminate cumbersome management procedures that must be manually monitored and maintained.

- **Increased backup consistency.** Cloud-based backup easily institutes policies that govern backup processes and access control. For many SMBs that have not engaged in more rigorous backup activities, this provides confidence that backups are being done efficiently and properly. Establishing particular levels of service can be well defined through service-level agreements (SLAs).

- **Accelerated implementation time.** Given the dynamic nature of the cloud-based delivery model, a backup solution can be implemented almost instantaneously.

- **Increased data security and reliability.** Through very predictable and well-established access control processes, data security and reliability can be dramatically improved. This will be increasingly important for SMBs that might have more stringent security requirements, such as accounting and legal firms or medical and dental offices.

Considerations in Choosing Cloud-Based Backup

As the promise of cloud-based backup unfolds, the market has been flooded with many service providers offering solutions for customers in consumer and commercial environments. However, not all solutions are created equal. A distributed backup system that can protect both centralized storage and endpoint workstations and laptops requires the following elements:

- **Automatic and simple —** a solution that "just works," with coverage of all protected endpoints, requiring no intervention from administrators or end users

- **Offsite storage —** to ensure backups and data are not affected by onsite catastrophes

- **Centralized management —** to control distributed systems and user access

- **Scalable management —** that does not become geometrically more difficult with the increasing size of the organization or increasing volumes of data

- **Application-specific protection —** for business-critical applications, such as Exchange and SQL databases

- **Rapid onboarding options —** because bandwidth limitations can delay comprehensive protection for firms with large, inadequately protected data sets

- **Secure and reliable —** must address specific security concerns through encryption and access control policies

- **Standards compliant —** many professions and industries require that storage providers' processes and procedures meet or exceed the strictest control objectives, as with SAS 70 auditing or ISO certification

Ultimately, customers are looking to deploy cloud-based backup solutions that not only provide data protection in a distributed environment but also address their concerns regarding trust, cost, and control. One such provider that has been developing its solutions around these themes is Mozy.

The Advantages of MozyPro Online Backup

EMC acquired Mozy in 2007, which means that Mozy has full access to EMC resources and assets. As a comprehensive solution, Mozy offers simple, automatic, and secure online backup specifically for desktops, laptops, and servers. Mozy has the experience, infrastructure, and financial backing to ensure that an organization's data is safe, secure, and available when needed.

Founded in 2005, Mozy is one of the most trusted online backup services for consumers and businesses. MozyHome is designed for consumers, while MozyPro is engineered for the SMB and enterprise segments. The company has more than 3 million users and 70,000 business customers backing up over 70 petabytes of information to multiple datacenters around the globe. Mozy is headquartered in Seattle, Washington, with offices in Pleasant Grove, Utah; London, England; Cork, Ireland; and Shanghai, China.

The overarching principles that drive Mozy's cloud strategy include:

- **Data protection for the entire organization.** A single backup solution that spans centralized servers as well as distributed PCs, laptops, and other mobile devices will provide business continuity for the entire workforce that is simple to manage and control.
- **Don't think about backup.** Backup should be set up once and then work automatically.
- **Files should be encrypted.** Backup files should be encrypted and stored in a secure, remote location that's accessible only to identified users — from anywhere.
- **Backups should be smart.** A backup system should be smart enough to back up only data that has not already been backed up, back up only parts of a file that have changed, and back up open and locked files.

Benefits of MozyPro Cloud-Based Backup

The MozyPro online backup solution for business addresses distributed data protection and the trust, cost, and control concerns of organizations looking to deploy cloud-based backup.

In particular, MozyPro offers:

- A single service that supports backup and business continuity across a distributed environment of multiple devices (PCs, laptops, and servers) among a variety of applications and server environments (including virtualized environments)
- Centralized and scalable management, leveraging a very simple and automated management scheme that is attractive to organizations with few to no IT resources
- A trusted provider that leverages the benefits and longevity of EMC
- A low-cost, subscription-based pricing model that allows low barrier to entry and long-term operational efficiency
- Enhanced security options including data encryption where key management is with the client (In addition, Mozy datacenters employ top levels of physical security based on SAS 70 and ISO certifications.)

- Hybrid cloud solutions incorporating EMC's Iomega line of entry-level, disk-based storage appliances (The ability to offer an integrated solution that spans both on- and off-premises locations affords users the benefits of consolidating local backup and increasing performance to accommodate first backup and full recovery, if needed.)

- Assessment services and guidelines to help customers understand how much data is to be backed up and the bandwidth considerations to accomplish the backup

CHALLENGES/OPPORTUNITIES

Several years of IDC research has highlighted that firms have two chief concerns with any public cloud service — data privacy and security. A firm's careful consideration of a supplier's implementation can alleviate these concerns. Factors such as encryption, key management, privilege access and logging, audit trails, SAS 70 auditing, ISO 27001 certification, data locale, and data breach handling should all be vetted. Firms such as Mozy with established security practices and offerings and strong financial and reputational strength can parlay these concerns into competitive advantage.

CONCLUSION

The practical reality is that SMBs and branch offices of larger organizations are recognizing the importance of protecting against data loss and providing business continuity among a distributed workforce. Constrained IT budgets, limited or no internal technical personnel, and a recognition that IT is not the core competency of the organization are driving these firms to consider and implement cloud-based storage services. New, comprehensive cloud-based approaches to data protection and data sharing functionality, such as MozyPro, introduce a cost-effective, simple, and predictable way for these companies to provide the business continuity that is fast becoming imperative to reduce risk.