

WHITE PAPER

Online PC Backup: Key Criteria in Selecting an Enterprise Solution

Sponsored by: Iron Mountain

Laura DuBois
December 2008

EXECUTIVE SUMMARY

Laptops and desktops, once forgotten corporate information assets, now need to be centrally protected and secured. IDC research suggests that achieving this goal will require increased spending on online PC backup services for centrally controlled protection, security, and discovery of data on corporate laptops, desktops, and mobile devices. This paper looks at the need for laptop and desktop data protection and, based upon recent IDC research, the key requirements firms should consider in evaluating enterprise-level online PC backup solutions. Iron Mountain has been a thought leader in the online backup market and serves small to large enterprise accounts with a PC backup solution.

Over the past few years, there has been a shift in the priority that enterprise firms give to protection of data on workstations, desktops, and laptops. Traditionally, the protection of data on laptop and desktop assets has not been performed by an IT organization, if at all. One approach was for resource-constrained IT organizations to rely upon end users to copy data to network shares. But any manual IT task left to a user to perform runs the risk of not getting done. Another option was making use of folder-level synchronization between a user's local files/directories and a centralized file server. Lastly, many users created their own backups, burning their local data to removable media (Zip, CD, DVD, Flash), which increased the risk of potential compromise. Each approach caused a unique set of challenges, from nonexistent backups and thus nonrecoverable data to lack of centralized control and inconsistent policy enforcement.

For most enterprises, there were no centralized backup processes for protecting user data on endpoints in a consistent and reliable fashion. IT organizations were focused on dealing with the unsolved datacenter issues of missing backup windows, troubleshooting failed backup jobs, monitoring performance and tape drive/media utilization, and keeping up with compressing recovery requirements. Discrete business units and C-level executives are now asking IT organizations to take on the protection and recovery of increasingly distributed data in a more consistent, repeatable, recoverable, centralized, and enforceable manner. Older or nonexistent approaches are no longer acceptable. What is driving this change in policy, strategy, and approach?

Risk mitigation and governance, risk, and compliance (GRC) initiatives. Large enterprise firms face different regulations for how they manage their company information. Electronic discovery of locally stored employee information, either in file directories or in local archives (PST/NSF files), is also a concern. Both drive the need for centralization of data for better information governance. Large enterprise accounts have formed GRC programs to effectively develop, monitor, and manage corporate information assets in a consistent, repeatable, and legally defensible manner. User data on PCs that is not protected, secured, and retained according to policy, while also discoverable, introduces risk.

Centralized management of distributed IT infrastructure. As consolidation in the average number of enterprise datacenters continues, the number of regional, branch, and home office locations expands. This expansion is being driven by the need for closer proximity to the customer, globalization, telecommuting, offshoring, outsourcing, and other business megatrends. With this increase in distributed business operations comes the need for greater control over and centralized management of distributed systems and data. This is true for servers in regional computer rooms and for laptops in branch and/or home offices. Backup of PCs and servers in remote or branch office locations is now being done from a centralized point of control, by IT staff, within the datacenter.

Compromises to sensitive corporate information on PCs. Incidents of loss of sensitive corporate information resident on laptops can damage a corporate brand, affect shareholder confidence, or increase customer and/or employee concerns about data privacy. The removable nature of laptops places this corporate asset at a high degree of risk for loss or theft. If the data resident on the asset is not encrypted and backed up, firms can face loss of or compromises to corporate information as well as worker productivity losses. This is driving firms to backup not only to protect against data loss and mitigate risk associated with potential data privacy breaches but also to encrypt data resident on removable devices.

Need for central visibility into distributed information assets. In the event that a laptop is lost or stolen, a centralized backup store is imperative in helping a firm understand the scope of potential information exposure. Moreover, firms can use a centralized, up-to-date backup store of distributed data to understand legal exposures. Integration of laptop backup with legal discovery and review tools can help reduce custodian discovery costs and plan for early case assessments.

The availability of online backup services for outtasking of PC backup has made it more viable as an IT service. Despite improvements in datacenter backup technologies, challenges still exist. These challenges stymie an IT organization's ability to take on new projects, in particular with limited IT staff. The increasing availability of online PC backup services makes endpoint protection more viable. Firms can increase their scope of protection and reduce their risk while only very marginally affecting capex and opex budgets while enabling IT datacenter staff to focus on management of information rather than infrastructure. What is online PC backup?

Overview of Online PC Backup

Online PC backup, also known as remote or Internet backup, is a method of offsite data storage in which a PC's files or folders or the entire contents of a hard drive are regularly backed up over the Internet (or a point-to-point connection) to a remote server within a third-party service provider datacenter. The PC backup can be done frequently (or continuously) to provide a second copy in the event of data loss (e.g., disaster, theft, virus, corruption, hardware failure). Encryption and password protection help to ensure privacy and security.

The top-level benefits to an online PC backup approach over an on-premise implementation include:

- ☒ **Budget relief.** No capital infrastructure or capital is required (e.g., servers, software, storage, training) to implement the offering.
- ☒ **Predictable spending.** With predictable monthly or quarterly billing costs, the service is amortized over a contract period based on backed-up capacity.
- ☒ **IT outtasking.** Online backup approaches significantly reduce the amount of time IT staff are involved in tasks such as backup. Backup configuration, troubleshooting, monitoring, and capacity planning tasks are eliminated.

There are a number of commercially available online PC backup solutions, some targeted at consumer and/or small office/home office (SOHO) environments and some architected for carrier-class volumes of PCs for the largest enterprises. Of course, the needs of a consumer or small office/home office will be considerably different from the needs of larger businesses and corporations. It's important to consider what types of services are needed, what types of systems and applications need to be protected, and the different backup policy, security, and services around recovery that are required. IDC research suggests the needs and requirements of consumers and small business owners for PC backup are quite different from those of the largest banks, healthcare providers, sales organizations, and enterprise institutions.

Table 1 provides a high-level comparison of the differing needs of consumer/SOHO and midsize to very large business users for online PC backup services.

TABLE 1

Comparison of Consumer/SOHO and Enterprise Business Users' Online Service Needs

Criteria	Consumer/SOHO	Enterprise Business
Use cases for online services	Backup only	Backup, disaster recovery, business continuity, ediscovery, long-term retention
Platforms	PCs only	PCs, application servers, file servers
Operating systems	Windows only	Windows, Unix, Linux
Content for online backup	File data only	Structured/application data and file data
Online PC backup configuration and management	By end users	Centralized policy for configuration and ongoing management by IT
Frequency of online backup	One time a day or more	Continuous to multiple times a day
Top online backup features	Ease of use	Pricing, rapid recovery option, security features

Source: IDC, October 2008

Table 2 goes into further detail on the most important criteria among firms of different sizes in considering an online backup service provider.

TABLE 2

Features Influencing a Business' Use of a Specific Online Backup Solution

Q. On a scale of 1–5, how much did the following features influence your decision to evaluate and/or implement a particular online backup solution? (1 = most important and 5 = least important)

	Total
Attractive pricing	2.02
"Rapid recovery" option using onsite appliance or quick-ship service	2.26
Security features within the service (encryption, etc.)	2.38
Ability to satisfy long-term retention	2.38
Quality of customer support	2.41
Ability to add storage capacity if needed over the course of the contract	2.43
Provider's ability to help with setup and configuration	2.50
Management GUI or portal that allows for monitoring and management of backups	2.54
Ability to customize service-level agreement (SLA) elements to our specific needs	2.57
Other	3.06
n =	473

Base = respondents who are in the process of considering, implementing, or currently using online backup

Note: Data is weighted by company size and vertical.

Source: IDC's *Storage as-a-Service Commercial Survey*, July 2008

Enterprise Requirements for Online PC Backup

In addition to differences in security, recoverability, systems/content coverage, and data privacy requirements, small and large enterprise accounts need to consider the following best-in-breed capabilities when evaluating online PC backup solutions:

- ☒ **Centralized management.** Unlike consumer-grade PC backup, which is configured by each distributed user, enterprise-level PC backup often dictates a centralized backup policy be applied consistently to all PCs. This centralized approach requires that distribution and installation of any PC-resident software be done in a silent (user-unassisted) fashion. Ongoing backups and monitoring of the backup completion must be equally transparent to the user. IDC research suggests solutions requiring user backup activation will not get done.
- ☒ **Reliable, granular, and system-level recovery.** If PC data is not recoverable, why back it up at all? Enterprise-level online PC backup solutions provide reliable restores by offering resumed backup for conditions that cause a backup interrupt (network disconnect). Some consumer-grade PC backup solutions require a middleman (IT help desk) to restore a file, while enterprise-scale solutions offer user-level, self-service recovery. This means a user can select and pull down files from a Web interface without help desk involvement. In the event that a system is lost or stolen, enterprise-level online PC backup can provide for cross-system recovery to a net-new PC device. Enterprise solutions need to offer system-level protection to recovery from a drive failure or if a PC is lost.

- ☒ **Use of data optimization technologies.** IDC research suggests that data growth averages 52% year over year. However, network capacity is limited. Enterprise solutions must include software features that reduce the amount of data sent over a network or stored at a third party by making use of data reduction technology for network and storage capacity-efficient backups. Moreover, an enterprise solution should offer centralized network bandwidth utilization by throttling back used network capacity during peak network times.
- ☒ **Backup handling.** Enterprise online PC backup solutions must provide clean, consistent backups of open files such as PSTs/email files, Word documents, and the like. Enterprise solutions should offer both scheduled and continuous backup capabilities to minimize data loss as well as resumed backups to pick up where a backup might have left off in the event of some form of backup interrupt.
- ☒ **Security.** The number 1 concern for firms in considering an online service is security and data privacy. Requirements for security include encryption of data not only in flight (in both backup and restore) but also at rest, including encryption of path names and directories. Security in an enterprise solution must also take into account physical and logical security within the third-party provider datacenter. Access controls and auditing should be reviewed for potential data breaches. Employee screening should be conducted. Physical security should include biometric access controls.
- ☒ **Architectural considerations.** In selecting an online PC backup solution, enterprises need to consider the scalability of the solution. How many PCs can be managed under the service in a centralized manner? Is the data protected in multiple, geographically distributed locations by the third-party provider for full failover redundancy of the backup service and recovery of the data? Datacenters should be Tier-4 SAS 70 certified.
- ☒ **Compliance/litigation readiness.** Large and very large firms in certain industries such as oil/gas, financial services, and healthcare/pharmaceuticals can face an average of three to four new legal matters per week. This typically involves preservation and collection of data on desktops and laptops. Online backup services can be used to provide a consistent, ongoing, metadata-preserved collection of PC data to comply with litigation holds and discovery/review. The service must be designed to conduct this collection in a legally defensible manner without modification to associated metadata.
- ☒ **Reliability of the supplier and the service.** IDC research suggests the number 1 criteria in selecting one online backup service provider over another is the reliability of the vendor and the solution. Enterprise firms should look for suppliers with a proven record in providing online services, developing multitenant shared software, and designing a common infrastructure. Offering services that make use of a shared infrastructure requires different expertise, process, and design.
- ☒ **Geographic support and localization.** Larger multinational firms with offices in non-English-speaking locations must consider solutions based on Unicode that offer local language support (or can be easily localized). The product user interface should be localized to support the top languages used by users and include proper handling of backups that cross time zones and country-specific day/date formats. However, it's not enough to offer only language support. The supplier must also offer sales, service, and support in region.

- ☒ **Flexible delivery model to meet enterprise requirements.** IDC research shows that the second-order concern firms have with deploying an online service is that the price will not justify a change from their current approach. Enterprises with this concern should consider suppliers with a hybrid approach where the same software can be deployed in an on-premise licensed software model, an online service model, or a combination model (remote managed service). As a firm's needs change, disruption to existing configurations are minimal.

IRON MOUNTAIN: THE CONNECTED BACKUP FOR PC SOLUTION

In 1995, Iron Mountain recognized the need for protecting enterprise data on PCs and pioneered the backup technology necessary to safeguard desktop and laptop data. Iron Mountain's Connected Backup for PC solution offers automatic desktop and laptop data protection and recovery. The solution eliminates the risk of PC asset or data loss by automatically and user transparently backing up PC data. No user involvement is required, which means users can go about their normal work-related tasks without being impacted.

Iron Mountain Connected Backup for PC Overview

Iron Mountain's Connected Backup for PC solution eliminates the risk of data loss, either logical or physical, from enterprise desktops and laptops, either LAN or WAN connected. Backup is done in the background and is transparent to users. On the need for recovery, a secure Web portal can be used to pull down select files or an entire system — without the need to involve the organization's help desk. The solution encrypts the data, in transit and at rest, using 128-bit AES encryption.

Connected Backup for PC can be deployed in one of three modes: *subscription (or online services)*, *licensed software*, or *remote managed services*. A *subscription service* uses Iron Mountain's secure offsite locations to back up enterprise data for a monthly usage-based fee, with no capital investment. A *licensed software* approach runs the Connected Backup for PC solution inside the enterprise IT environment. Iron Mountain Professional Services is available to help install and configure the software. Lastly, with *remote managed services*, Iron Mountain remotely manages the licensed software at an enterprise's datacenter.

The Connected Backup for PC solution offers the following features:

- ☒ **Self-healing backup.** Using cyclical redundancy checks (CRCs), the solution scans for corruption and repairs damaged applications, configurations, and files on any PC before backup.
- ☒ **MyRoam.** This Web-based access portal lets users access their backed-up data anywhere, without IT intervention.
- ☒ **Centralized, administrative console.** IT personnel can manage and monitor backup policies from a central console, over a corporate network or the Internet.

- ☒ **Network bandwidth throttling.** Bandwidth throttling gives IT control over upload bandwidth so that backups don't interfere with other high-priority tasks.
- ☒ **Secure, third-party facility.** Subscription service customers have the protection of Iron Mountain's underground vaults with 24 x 7 armed security, level 4 security rating, BRUNS-Pak rating of 9, and an OSHA-certified fire company to ensure data security.
- ☒ **DeltaBlock.** This feature sends only the changed data in files, saving transmission time and storage requirements. When a document changes, DeltaBlock only backs up the changes at the block level. This technology reduces backup time, minimizes network traffic, decreases storage, and enables backup over low-bandwidth connections.
- ☒ **SendOnce.** This patented technology eliminates duplicate files by saving each file only once. Files are backed up to a SendOnce pool, preventing identical copies from being stored in multiple user archives.
- ☒ **Connected EmailOptimizer.** This facility reduces the storage space for email files by 30%. This optional service recognizes duplicate email attachments and stores them only once, significantly reducing storage requirements.
- ☒ **Encryption.** The solution makes use of secure 128-bit AES encryption. Enterprise data remains encrypted both during transmission and in storage.
- ☒ **Integrated backup and security.** An optional PC Data Protection Suite packages the Connected Backup for PC solution with Iron Mountain's DataDefense solution. The DataDefense solution intelligently encrypts and automatically eliminates compromised data on a lost or stolen laptop or PC.
- ☒ **Connected DiscoveryAssist.** This solution allows an enterprise to gain access to and retrieve data across all repositories in Connected Backup Data Centers. Connected DiscoveryAssist offers path and file name filtering to speed data collection and maintains the file metadata necessary to support third-party search and review. This can dramatically reduce time and cost during ediscovery.
- ☒ **Other features.** Localization with support for 14 different languages, published database schema for use with third-party reporting tools, checkpoint restart on backups, VSS integration for open file backup, support for Windows and Mac OS operating environments, and VMware ESX support for VMDK file backup.

CHALLENGES

In a recent study on online backup adoption, 52% of 810 businesses surveyed indicated that they plan to evaluate or consider online backup in the next 12 months. For those firms with no plans to consider online backup, IDC research suggests that the inhibitors to deploying online services are data privacy and security concerns and the perception that the cost savings in using online services did not justify a change from current on-premise methodologies. A third-order concern was loss of corporate control over their IT processes and a break from corporate culture.

While Iron Mountain can address many of these concerns, it will take time for some business entities to overcome these barriers. However, given the increasing legal and regulatory pressures to secure and protect endpoint data and the current economic climate, the business and budgetary advantages over time will likely outweigh any technical concerns, and compressing IT budgets will drive out cost/benefit barriers.

CONCLUSION

IDC finds Iron Mountain to be in an advantageous position with its storage-as-a-service offerings, which provide a breadth of services from PC to server backup, archiving, ediscovery, and records management. We expect the trend for increased spending on backup of remote and distributed PC assets to continue and more firms to evaluate and procure online PC backup services for central control protection, security, and discovery of distributed data on corporate laptops, desktops, and mobile devices. IDC recommends enterprise accounts considering online PC backup services evaluate at length potential suppliers to ensure their security, reliability, and recovery requirements for user data can be met according to agreed-upon service-level agreements. Iron Mountain, an early thought leader in the online backup market, should be on a firm's short list for consideration.

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 2008 IDC. Reproduction without written permission is completely forbidden.