
Continuous Data Protection and Instant Recovery for Laptop computers

For the past decade, IT organizations have focused their efforts on protecting information residing within the walls of their data centers. However, today's increasingly mobile professionals are replacing their desktop PCs with laptop computers making it increasingly difficult for IT administrators to consistently back up, safeguard and quickly recover business critical data stored beyond the firewalls.

With the ongoing focus on data security, compliance and disaster recovery, IT administrators are being challenged to comprehensively protect their organizations data assets regardless of where the data resides. This white paper addresses the unique challenges posed by mobile users, and introduces a proven low cost, real time data protection and instant, self-service recovery solution specifically designed for Windows laptop and remote office PCs.

Executive Summary

IT Managers are faced with a daunting challenge when it comes to protecting corporate data. Not only is data growing at unprecedented rates, but it is also growing increasingly mobile. More and more companies are equipping their sales teams and executives with laptop computers, making it increasingly difficult for IT administrators to consistently back up, safeguard and quickly recover highly sensitive data stored on the hard drives of their employees' laptops.

Why should you be concerned?

Your corporate data is at risk: Analysts estimate that over 70% of a company's data now resides outside managed servers on laptops computers and individual desktops. In addition laptops are facing a host of new threats; including thefts, hardware failures, and data corruption, further exposing your organization to considerable legal and financial risks.

Your current data protection policies are most probably ineffective: Most organizations rely on their mobile users to manually copy business critical information stored on the hard drive of their laptops to a network server. Unfortunately, studies have shown that backup and data protection policies are rarely followed and scheduled backup times are missed, leaving sensitive data unprotected and your organization exposed to irreparable data loss.

Restoring from days, or even hours, ago no longer gets your organization back in the game. Today's business climate demands 24/7 access to data whether users are on or off the road. Mobile users also demand faster and more granular file recovery, including rolling back to previous versions of critical documents stored on their laptops.

While traditional disk and tape backups have proven effective for years to protect corporate information residing within the walls of data centers, most IT managers have come to realize that their current policy and infrastructure is no longer reliable when it comes to protecting, safeguarding and recovering their distributed corporate data. Further, the recreation of lost data is frustrating, time consuming, very expensive and adds extra burden on already taxed IT departments.

With over one-half of all new corporate PCs purchased in 2008 expected to be laptop computers, the need for a low cost, fast, easy, secure and fully automated solution that provides laptop PCs real-time, 24/7 data protection and mobile users self-service recovery is quickly becoming a top priority for IT executives.

With its innovative continuous data protection and right-clickable recovery, EMC is leading the industry by empowering laptop – and remote office users - with instant, self-service recovery capabilities and IT administrators with peace of mind data protection insurance.

Key Facts:

10% of an organization's laptop will suffer a catastrophic data loss each year. Each data loss event costs on average \$3,957

Source: Pepperdine University Study

“Only 25% of the organizations have an effective solution in place to protect and recover information stored on their laptops and desktop PCs” Source: Enterprise Strategy Group Study

Key Laptop Data Protection and Recovery Challenges

For most employees today, working from 9 to 5 in an office is a thing of the past. Equipped with laptop computers, many individuals are now working around the clock while seated in an airport lounge, at a local Starbucks, in a remote office, or simply at home. For those mobile users, accessing their files at any time is priceless. However, for IT administrators tasked with safeguarding corporate data, these mobile employees pose new data protection and recovery challenges while introducing increased legal risks and potentially sizeable costs to the organization.

Increased mobility means increased risk

Today, mobile users are more easily accessing and exchanging business information. As a result, valuable corporate data which was once tightly secured within the networked perimeter is now primarily stored on the hard drives of mobile users' laptops. In fact, analysts estimate that over 70% of the company's data resides outside managed servers – most of the time unprotected and therefore vulnerable to data loss and corruption.

For the average business, whatever its size, the impact of lost data is, at a minimum, an inconvenience; at worst, it is a critical blow to daily operations. In all cases, it means lost productivity. For the laptop user, it usually means frustration and waiting, hoping that the lost file was saved 'by chance' on a backup server. For the IT administrator, already struggling to keep up with the exponential growth of corporate data, the re-creation of the lost data always means headaches and extra work.

Data loss events are primarily caused by hardware failures, human errors (accidental file deletion or file overwrite) and corruption caused by virus or hacker attacks. Not only do data loss events hamper productivity but they also seriously impact the bottom line. According to a recent Pepperdine University Study, the average organization can expect to experience a 'catastrophic data loss' event on approximately 10% of its laptops during the course of the year. Each data loss event, costs an organization an average of \$3,957 in lost user productivity, IT support costs, and replacement costs. (Note that this estimate does not even take into account any lost opportunity resulting from critical data loss such as prospects contacts accidentally deleted.)

Key Facts:

“A single stolen laptop can cost a company more than \$6,000 for hardware, software, restoring data (assuming it was backed up in the first place) and user downtime. This number does not even account for the cost of any data lost or exposed”

Source: Gartner

And, because laptops are more easily lost or stolen, the risks are even greater, further exposing organizations to considerable legal liabilities and financial risks. As a matter of fact, more and more businesses are now legally required to formally extend data protection to laptop computers in order to comply with data privacy laws and other key regulations such as California's SB 1386 and HIPPA.

Unfortunately, while almost every organization has a system in place to protect data stored on network servers and mainframe computers, very few have successfully extended this protection down to information stored on

their laptops – leaving some of their most sensitive corporate data unprotected and their organization exposed to irreparable data loss, additional costs and tight legal scrutiny.

Increased mobility also means increased dependency on end users

Traditional Retrospect backup software typically runs once a day and takes a ‘daily snapshot’ of the files stored on a PC. However if a user is traveling or if his laptop is powered off when the daily backup is performed, his laptop computer is skipped.

It’s no longer enough to back up data periodically. The most valuable files are usually the ones that mobile users have worked on most recently. That means that organizations only backing up data once every 24 hours risk losing eight or more hours of their employees’ most recent — and therefore most valuable — output.

To solve this problem, many organizations have resorted to ineffective, ad-hoc solutions to protect the data stored on their mobile users’ laptops. The most common approach has been to create network shares and instruct their users to manually copy their data onto these shares. However, this policy has met with only limited success and many IT administrators readily admit that most of their mobile users do not adhere to any data protection policies because they are not enforced.

Laptop users simply cannot be relied upon to routinely back up their own data, leaving highly sensitive information unprotected. It’s no surprise, then, that the protection of laptops has become a top priority for many businesses — especially medical practices, financial institutions and other small and medium size businesses.

Key Facts:

“Human error – primarily accidental file deletion or modification – causes between 33 to 40 percent of all data losses. Research also shows that up to 97% of all "restores" are single files, causing huge burdens on IT personnel and lost productivity while users wait” Source: Microsoft

“The truth is you can backup all the data you want but if you can't recover it, it doesn't do any good, because it is recovery that end users actually seek. In the end, backup doesn't matter, recovery does” Ray Paquet, Gartner

End users demands for faster, instant recovery

Today’s business climate also demands instant, on-demand recovery. Restoring from days, or even hours, ago no longer gets mobile users and companies back in the game... Laptop users want to have access to their files at anytime, whether they are working online or offline. In fact, they don’t really care whether or not their files are protected. What they really care about is the quick recovery of any of their files should these get inadvertently deleted or lost. They also want more granular file recovery, including rolling back to previous versions of critical documents stored on their laptops.

IT administrators need a 24/7 real-time backup and recovery solution for their laptops that provides them peace-of-mind data protection insurance while allowing mobile users to self-restore any deleted, modified or corrupted files. Ultimately, the ideal solution should:

- a. Prevent any data loss whether laptop users are working online or offline
- b. Empower the user himself to recover any accidentally ‘lost’ data stored on the local hard drive of his computer

- c. Prepare the organization for any regulatory scrutiny while easing the overall data management and reducing the total cost of ownership

Solving the Laptop Data Protection and Recovery Dilemma

Introducing Continuous Data Protection Technology

Continuous data protection (CDP) is a relatively new storage technology in which all the user data in an entire company is backed up whenever a change is made. In effect, CDP automatically saves a copy of every change made to a file, by creating an electronic journal of complete file changes, essentially capturing every version of the file that the user saves. If a computer or the network become infected with a virus or Trojan, or if a file becomes mutilated or corrupted and the problem is not discovered until some time later, CDP allows recovery to the most recent clean copy of the affected file.

By delivering better recovery-point capabilities, CDP provides more granular and resilient data recovery solutions than traditional backup software. It eliminates the need for full, incremental, or differential backups currently in place – protecting data immediately and continuously by backing it up to disk. It also allows end users to restore their own data to any point in time within minutes or seconds ... and without contacting IT.

Ultimately CDP allows IT organizations to get back in business quickly while minimizing the loss of data.

Key Facts:

“Continuous Data Protection (CDP) is a methodology that continuously captures or tracks data modifications and stores changes independent of the primary data, enabling recovery points from any point in the past” Source: Storage Networking Industry Association

Addressing the Laptop Data Protection and Recovery Challenges

Most importantly, CDP also addresses the specific data protection and recovery challenges with laptop data. CDP can be used to journal file changes on the mobile user's local hard drive and automatically upload them to a central server whenever the user connects to the office network. If a laptop is offline, changed files are stored on the local disk and then copied to the file backup locations when users reconnect to their network.

With this in mind, IT organizations need a secure, real time CDP solution that

- Provides 24/7 mission critical business continuity protection for laptops by automatically tracking changes as they occur and securely backing up the most critical files

- Provides IT Managers with a powerful file protection and restore solution transparent to end users, easy to deploy, easy to manage and fully scalable

- Provides end users - whether online or offline– with instant, self-service file access and recovery by rolling back to any previous versions and/or deleted files - without any IT administration intervention

- Provides organizations with a cost effective and reliable solution that allows them to effectively manage their mobile users' data integrity and availability and prepare them for any regulatory scrutiny and/or legal requirements

Continuous Data Protection and Instant Recovery for Windows PCs

Until now, the relatively few companies that did systematically back up their laptop data could only do it on a periodic basis, usually every 24 hours. This method leaves mobile users' most recent and valuable work unprotected. With Retrospect Continuous Backup, your most sensitive corporate data is no longer at risk.

EMC Retrospect Continuous Backup is designed specifically to address the mobile users' data protection and recovery challenges by working in conjunction with traditional scheduled backups, adding Continuous Data Protection for Windows laptops and remote office PCs.

Retrospect Continuous Backup enables organizations to:

- a. Continuously protect key corporate data stored on Windows laptops and remote office PCs including Microsoft Office documents, email, calendaring information and contact databases.
- b. Empower mobile users with instant, on-demand right clickable recovery, allowing them to recover their own data files and/or any previous versions of any document without IT intervention
- c. Avoid/reduce the financial impact of data loss associated with lost/stolen laptops and hardware failures
- d. Ensure data integrity compliance with key Government regulations such as Sarbanes-Oxley and HIPAA and data privacy laws (such as California's SB 1836)
- e. Lower IT operating costs by extending any organization's existing backup and recovery systems and by empowering end users to recover their own files while easing the burden on help desk staff.

Retrospect Continuous Backup @ Work

Consistently protecting and quickly recovering highly sensitive data stored on Windows laptop and remote office PCs has never been so easy, fast and secure. Retrospect Continuous Backup already provides many organizations with a 24/7 low cost, yet powerful, real-time data protection and recovery solutions for Windows laptops and remote office PCs.

Transparent CDP for Windows documents

Retrospect Continuous Backup automatically backs up documents in real time as they are saved to disk regardless of whether their documents are stored on a laptop, remote office desktop, on a network file server or attached storage device. Documents are first backed up to a data repository that resides on the local hard drive of the Windows PC being protected. When the PC reconnects up to its network, Retrospect Continuous Backup automatically replicates the protected files to one or more file servers or Network Attached Storage devices. Retrospect Continuous Backup operates transparently and does not require any actions on the part of the end users.

Retrospect Continuous Backup Architecture

Retrospect Continuous Backup combines a lightweight desktop agent with a central management server to provide a scalable, policy-based system to protect every Windows laptop, remote office PC and desktop in the company.

Retrospect Continuous Backup agents protect every file a user creates, modifies and saves on their Windows laptop according to data protection policies defined on a central Continuous Backup Policy Server. Administrators access the Policy Server via a browser-based console. Using the console, administrators can centrally define company-wide policies for file protection, versioning, back up and retention. The Retrospect Continuous Backup Policy Server also provides administrators and auditors with a robust set of reports that provide information regarding agent activity, policy compliance, etc.

The Retrospect Continuous Backup storage locations are specially protected directories that reside on file servers or Network Attached Devices that store the data backed up from mobile users' laptop and remote office PCs.

Back up what's important, skip what's not

By design, Retrospect Continuous Backup only backs up the irreplaceable data files that reside on a user's Windows PC. Replaceable files such as the operating system, application files, etc. are not backed up, which reduces the amount of network bandwidth and storage required to protect a large organization's PC population. Additionally, administrators can define policies to specify which file types are backed up – e.g. Microsoft Word documents, Visio drawings etc – and which files to skip – e.g. MP3 music files, etc.

“Always open files” Protection

Protecting files that stay open during a backup operation has always been problematic for traditional backup software. The classic example is backing up emails and calendaring data stored in Microsoft Outlook Personal Folders (a.k.a. PST files).

Retrospect Continuous Backup Open File Protection technology performs hourly backups of open files while the files are in use. This hourly backup occurs automatically and is once again transparent to end users. In fact, Continuous Backup ensures that a ‘fresh’ copy of a users' email, desktop databases, etc. is always available for recovery.

Secure and encrypted data

The recent rash of lost and stolen back up tapes underscores the importance of securing back up data. Retrospect Continuous Backup provides administrators with the option to encrypt protected files while they are in transit over a network as well as at rest on a Continuous Backup storage location. Retrospect Continuous Backup also empowers auditors to safely search every data file created on the network and or stored on lost/stolen laptops, without relying on end users.

Superior mobile users' support

Retrospect Continuous Backup is specifically designed to protect and quickly recover Windows documents while on the road. Continuous Backup automatically detects when a user reconnects to their organization's network and automatically backs up files created and modified to a network file server, including the previous versions of those files. Users can also recover the current and previous versions of their files while disconnected from their corporate network.

In addition, Retrospect Continuous Backup only backs up the changes that occur to a file since the previous backup, minimizing the impact on the organization's network bandwidth and storage resources.

Company-wide, centralized data protection

Designed to deploy to 1,000s of laptop and desktop PCs, Retrospect Continuous Backup allows IT administrators to define and enforce data retention and backup policies company-wide. Continuous Backup also achieves a low Total Cost of Ownership by leveraging standard Microsoft technology including Microsoft IIS ASP.NET, Microsoft .Net Framework 2.0 and Microsoft SQL Server.

Point, Click and Recover your files in seconds with Retrospect Continuous Backup

According to Microsoft, 85% of all requests to recover lost/corrupted files are for a single file less than 30 days old. Traditionally these file restore requests have been serviced by IT departments, tying up expensive IT resources to perform tasks that can be performed by end-users.

With Retrospect Continuous Backup's right-clickable recovery, end-users can access the previous version of any file with a simple right mouse click. End-users are also a single right mouse click away from recovering recently deleted files. Continuous Backup enables IT departments to avoid the majority of single-file restore requests, reducing IT helpdesk call volume and thus lowering IT operating costs.

Conclusion

Continuously protecting and quickly recovering business-critical information is no longer an optional line item. It is mission critical for any competitive organization.

Up to now, IT managers have struggled to find an effective solution to protect the highly sensitive corporate data residing on distributed Windows PCs. Fortunately, Continuous Data Protection (CDP) provides the avenue to address the laptop and remote office PC challenges in a way that dramatically improves overall data protection and recovery without weighing down IT in costly, high administration solutions. In fact, demand for CDP is growing as more companies realize they not only need to capture data more frequently but that they also need to provide faster recovery with less data loss.

With its innovative continuous data protection, EMC Retrospect Continuous Backup is leading the industry by empowering mobile users with instant, self-service recovery and providing IT administrators with peace of mind data protection insurance. For any organization that wants to ensure laptop data integrity, data accessibility and compliance with key data privacy regulations, Retrospect Continuous Backup is the ideal solution. Retrospect Continuous Backup is a proven low cost, real-time data protection and instant, self-service recovery solution specifically designed for Windows laptop and remote office PCs.

For more information visit www.emcinsignia.com or call **877.222.5879** today.