IBM Global Services
January 2008

Solving the distributed data problem.

The rise of remote data protection services

Contents

Introduction

Companies need to reevaluate traditional methods of protecting branch office and PC data such as tape backups and other localized do-it-yourself solutions. The risks and potential costs of data loss, regulatory noncompliance and business interruptions are serious and escalating. The scope of the problem keeps growing as well, as more and more business-critical information is generated and stored at remote sites and on end-user computing devices.

On demand data protection services represent a reasonably priced, workable solution to a thorny problem. The market has matured, and service providers are aggressively expanding their offerings to meet an ever more diverse set of clients, making this an ideal time for companies to explore other options for protecting their data.

Threats to data security

Business data is on the move in more ways than one—and the result has been a major IT headache.

Threats to business continuance and data security keep growing—from hackers and hurricanes to internal threats from disgruntled or careless employees. Widespread disasters like Hurricane Katrina have shown all too clearly the dangers and weaknesses of localized backup and recovery.

Failure to retain critical information in a safe, secure, easily recoverable form has landed companies with multimillion dollar fines, not to mention serious losses in revenue, customer goodwill, market position, credibility and productivity.

Highlights

Savvy corporate decision makers have recognized that to deal with these challenges, they need to deploy a companywide data protection infrastructure. However, doing so in house can be prohibitively expensive, not least because more and more business information is being generated and stored outside the data center and beyond central I T control—at branch offices and on employee PCs and laptops. Protecting and managing this distributed data has become a major expense and challenge for corporate IT staffs.

To solve the problem, a growing number of companies are turning to an entirely different kind of solution: remote on demand data protection services.

Explosive data growth, increased risk

Managing and protecting distributed data has become a major challenge.

Businesses are responsible for protecting and securing an already extensive and rapidly growing body of information. Managing and protecting that data has become a major challenge for I T departments, as much of it is being generated outside of the corporate data center.

Protecting data across a distributed enterprise constitutes a huge and growing I T expense. Companies cannot afford to put the problem on the back burner: The dangers and potential costs are much too high.

Companies of all sizes are expanding to include more remote or branch locations.

The problem is likely to worsen over the next few years for companies of all sizes. Data becomes less centralized as businesses expand to include more remote or branch locations. Factors driving this trend include offshoring of business processes, supply chain integration, expansion into key regions for competitive purposes, mergers and acquisitions and market globalization.

Branch offices often lack adequate onsite I T support. With limited resources to focus on backup and recovery, properly managing and protecting data can be difficult.

Highlights

Unencrypted tapes are a security risk, as they are easily lost or stolen.

Backing up remote sites can be expensive and complex.

Tape backup: popular and problematic.

For sites with little or no local I T support, tape backup has become the de facto data protection strategy. However, this approach is unsatisfactory because it tends to be:

- *Unreliable and haphazard, posing the risk of being found noncompliant with federal, state, securities and business continuance mandates for companies of all sizes.*
- *Difficult to centrally manage, as I T staffs may not have a way to monitor remote operations to ensure that backups take place and are successful.*
- *Risky, with tapes easily lost or stolen, particularly in transit, as when they are being moved to a secure offsite facility.*
- *Capital and I T resource intensive, requiring servers, tapes, disk drives and backup software at every site.*
- *Slow and cumbersome, hindering the realization of recovery point objectives (RPOs) and recovery time objectives (RTOs).*
- *Unable to protect companies from serious data loss, lost productivity and regulatory fines that result from inadequate data protection.*

The data center dilemma.

Some companies are backing up remote sites to data center servers. However, this solution can be both expensive to deploy and complex to administer. Each remote site must be equipped with a networked storage device and replication software. Network costs increase as well, since periodic server backups tend to hog wide area network (WAN) and local area network (LAN) bandwidth, potentially interfering with business-critical transmissions and end-user productivity.

Highlights

Companies need to protect information that is being generated remotely.

Protecting end-user data

Branch offices constitute only one piece of the distributed data protection picture. Companies also need to protect the information that is being generated, downloaded and shared by a rapidly growing horde of PCs and mobile computing devices.

Today's mobile workforce generates massive amounts of data, often many miles away from corporate headquarters and I T control. Protecting and securing this critical and sensitive information, which includes client records and intellectual property, becomes the sole responsibility of these time-challenged and often nontechnical end users.

The need to protect this data is urgent: Computers can be stolen, suffer hard disk failures or become infected with viruses. While remote PC backup products are available, they tend to be bandwidth and CPU intensive, slowing down application and network response times, annoying users and negatively impacting productivity.

A viable alternative

This situation poses a serious dilemma for many corporate I T departments. They realize that their current distributed data protection setup is inadequate and that a centralized infrastructure is the best way to go but lack the resources to deploy and manage it in house.

An on demand distributed data protection service can provide increased reliability and security.

Fortunately, there is a better way to go: an on demand distributed data protection service that automatically backs up offsite PCs and servers with greater reliability and security, virtually anywhere on a client's Internet Protocol (IP) network.

Highlights

Remote on demand services have become the data protection solution of choice for many companies.

On demand data protection services offer hardware and software, centralized management and reporting, 24 7 monitoring and management, third-party hosting and offsite Tier 1 data facilities. Remote on demand services have become the data protection solution of choice for a growing number of companies of virtually all sizes.

The on demand data protection service model offers several major advantages over a do-it-yourself, in-house solution.

Evaluating ROI
When evaluating ROI for a service-based protection solution, a company needs to take into account all of the relevant costs that would accrue from deploying a comparable solution in house. An analysis should take into account probable increases in these costs over time, as the installation grows to meet increased demand. They include:

- *Capital costs, including storage network hardware, software and long-distance connections, as well as building facilities for a primary, and possibly a backup, data center*
- *Labor costs, including training existing staff and hiring new technicians to install, maintain and manage the new installation.*
- *Hidden costs that result from insufficiently protected data and systems (including, but not limited to, loss of I T and end-user productivity, lost revenue and customer goodwill and regulatory fines).*

On demand services may provide significant returns in both capital and labor costs.

On demand services may provide significant returns in all of the above cost areas. Equipment, software and technical support are provided as part of the service, helping to save the client on both capital and labor costs. The client pays by the month, according to how much data needs to be backed up.

Highlights

The right service provider can offer a level of distributed data protection that most companies cannot afford on their own.

High service levels, enhanced continuity.
What is most important is that the right service provider can help guard against the high costs of data loss by providing a level of distributed data protection that most companies cannot afford on their own. I T managers can rest easier if they feel that backups can take place on schedule across all branch offices and designated PCs and servers, and that RPOs and RTOs will likely be addressed. Data can be housed in the service provider's remote disaster-recovery facility, increasing business continuity if a disaster should take out a branch office or even headquarters.

Scalability
For most corporate IT staffs, keeping up with a company's growing data protection demands is a constant struggle as well as a major expense. On demand services have the built-in redundancy, capacity and flexibility to help address the needs of companies of nearly any size, and to scale up or down relatively quickly and smoothly when those needs change. Paying only for services used, a company no longer has the expense of purchasing and maintaining equipment that is often either under- or overutilized. As a further benefit, the on demand model helps IT administrators predict and plan for future costs far more accurately.

The on demand model helps IT administrators predict and plan for future costs far more accurately.

Established solutions demonstrate efficacy of the on demand model.
One such managed on demand data protection solution is IBM Information Protection Services—remote data protection service.

The remote data protection service helps companies protect data on servers, PCs and laptops across the organization.

This service helps companies protect data on servers, PCs and laptops across the organization and from virtually any location. Data is automatically backed up via the client's existing network to our security-rich offsite data centers.

Highlights

The remote data protection service is a pay-as-you-go subscription service designed to make data protection costs highly predictable and reasonably priced for clients. The service includes the hardware, software and operational support needed to quickly and more easily implement an effective data protection strategy. This approach helps eliminate the research, implementation, hiring and training costs of launching an in-house solution—while accelerating service delivery.

Daily backups are intended to be fast, cost-effective and convenient to provide consistent data protection.

Data is backed up automatically on a daily basis, facilitating extremely fast performance with fewer demands on clients' networks. It is intended to be a fast, cost-effective and convenient way to provide consistent data protection across an organization's servers, PCs and locations, while reducing the need to increase network investment.

The service can be cost-effective for businesses of nearly any size—from large global enterprises with multiple sites to small and midsize businesses (SMBs)—because clients only pay for the amount of data they back up.

Benefits of the remote data protection service

Clients can redeploy personnel to potentially lower their backup and recovery management costs.

- ***Increased potential for cost savings and ROI.*** *Equipment and support are provided for clients at disaster-resistant data centers, reducing the need for capital investments in hardware or software. Pricing is based on the amount of data clients protect, allowing them to control their costs because capacity utilization is improved. And because critical data protection operations are automated, clients can redeploy personnel to other projects and potentially lower their backup and recovery management costs.*
- ***Offsite data protection.*** *The remote data protection service supports reliable and efficient automated offsite daily backups of server and PC data for business continuity and disaster recovery, virtually anywhere data resides (branch offices, mobile devices, etc.).*
- ***Higher service levels and increased continuity.*** *Backup and recovery of vital business data are supported and managed 24 hours a day, 365 days a year.*

Highlights

With the remote data protection service, protecting and accessing data can be extremely efficient.

Our disaster-resistant centers are designed to protect client data from even the most extreme natural events.

- ***Nonintrusive, scalable backups.*** *Advanced technology reduces the bandwidth required to protect client data, helping to enhance computer and network performance. The remote data protection service includes a high-capacity infrastructure that addresses a client's changing needs as the amount of data grows.*
- ***Greater ease of use.*** *Intuitive applications and Web portal interfaces make it easier for personnel to back up and restore data automatically with a few mouse clicks.*
- ***Faster backups and recovery with no tape.*** *Tape solutions can be slow, frustrating and unreliable. With the remote data protection service, protecting and accessing data can be extremely efficient.*
- ***Flexible retention policies and long-term archiving.*** *The remote data protection service allows clients to define specific time-based data retention policies that match their business needs—from daily, weekly and monthly, to yearly retention options for compliance efforts. And the remote data protection service also offers the option to archive everything to tape for long-term retention.*
- ***Security and compliance.*** *The remote data protection service features 128-bit Advanced Encryption Standard (A E S) encryption, which tends to be more secure because it helps ensure that only authorized users can access data. In addition, our disaster-resistant centers are designed to protect client data from even the most extreme natural events, which is one of the safest alternatives.*
- ***Comprehensive platform support.*** *The remote data protection service features power-ful platform support for Microsoft® Windows®, UNIX® and Linux® operating systems as well as leading databases such as Oracle, Microsoft Exchange and SQL and virtual machines from VM ware, Microsoft and Sun.*

Highlights

Rapid onsite data recovery helps meet increasingly stringent RTOs.

To help reduce recovery time, an appliance with client data can be quick-shipped to the client's location.

Capabilities and options for server data protection

Remote data protection Onsite Appliance option for server data protection
The remote data protection Onsite Appliance option offers rapid onsite data recovery to help address increasingly stringent RTOs. This option is delivered through installation of a preconfigured storage appliance on the client's LAN, allowing a failed server to be recovered in hours rather than days.

Remote data protection Bare Metal Recovery option for servers
The remote data protection Bare Metal Recovery option is a managed and automated service that helps clients rapidly complete a "bare metal" recovery of their server operating systems and applications up to 80 percent faster than traditional methods allow. With this option, clients have a more reliable and cost-effective tool for bringing their business back online quickly.

Remote data protection Quickstart option for servers
The remote data protection Quickstart option is an onsite, security-rich data protection option for large enterprise branch offices or SMBs that can dramatically reduce the time and bandwidth typically required to complete an initial backup over the Internet. This is done by collecting a data copy locally and then shipping the data to the provider's service platform, where it is imported. Once the data is on the IBM service platform, incremental backups completed over the Internet can be performed in a fraction of the time typically required.

Remote data protection Quickrestore option for servers
The remote data protection Quickrestore option is a security-rich disaster recovery option for large enterprise branch offices or SMBs. In the event of a server or site disaster, an appliance with client data can be quick-shipped to the client's disaster recovery or original location to help reduce recovery time. Large server restore time can be cut substantially by reducing the need for large restores to be sent across the Internet.

Highlights

Data is automatically backed up on a daily basis.

Data can generally be backed up and restored at any time.

Capabilities for desktop and laptop PC data protection

For desktop and laptop PC data protection, the remote data protection service offers a managed online data backup and recovery service that addresses critical data protection, business continuity and financial requirements for both large enterprises and SMBs.

Data from a client's desktops and laptops is automatically backed up on a daily basis through the client's existing network connection to a security-rich offsite storage facility. Mission-critical data is centrally managed, more securely protected and more easily recoverable when it is needed.

Operationally, the remote data protection service is designed to be a fast and highly efficient solution. By transmitting only data that has changed since the last backup, the remote data protection service reduces the bandwidth required to perform these operations. This helps lessen the impact on individual computer and network performance, allowing clients' staff to continue working during the backup process. Data can generally be backed up and restored by individual users at any time, without I T support, using the intuitive remote data protection user interface. Users log in to the application and simply select the data they would like to back up or restore. With the ability to select single files or entire folders, users can typically retrieve different versions of their files from any backup performed during the previous 30 days.

Summary

Companies need to reevaluate traditional methods of protecting branch office and PC data such as tape backups and other localized do-it-yourself solutions. The risks and potential costs of data loss, regulatory noncompliance and business interruptions are serious and escalating. And the scope of the problem keeps growing, as more and more business-critical information is generated and stored at remote sites and on end-user computing devices.

The remote data protection service can help to guard against the high costs of data loss by providing a level of distributed data protection that most companies cannot afford on their own. With several service options, on demand data protection services can be a reasonably priced solution for companies of virtually any size.

For more information

To learn more about IBM Information Protection Services—remote data protection service, contact your IBM representative, or visit:

ibm.com/services/continuity

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
01-08

BUW-03002-USEN-02