



Moving beyond tape backup

Addressing the data protection challenges for midsize businesses

Contents

- 2 Introduction**
- 2 Data protection challenges**
- 2 Under resourced and at risk**
- 3 Tape backup: popular and problematic**
- 4 Protecting end-user data**
- 5 A better alternative**
- 7 Established solutions demonstrate the efficacy of the on demand model**
- 10 Capabilities and options for server data protection**
- 11 Capabilities for desktop and laptop PC data protection**
- 12 Summary**

Introduction

Midsized businesses (with between 500 and 1,000 employees) need to re-evaluate the wisdom of protecting branch office and PC data with tape backups and other localized do-it-yourself solutions. The risks and potential costs – of losing crucial information for good, interrupting operations, losing clients and being found noncompliant by federal regulators – are too great. And the price of failure keeps growing, as more and more business-critical information is generated and stored at remote sites and on end-user computing devices. For many midsized businesses, on demand data protection services represent a reasonably priced, workable solution to a thorny problem.

Data protection challenges

Midsized businesses face the same basic data protection challenges as large businesses. The dangers and potential business costs of unprotected data can easily be catastrophic, whether a company runs on megabytes or terabytes of data. Unfortunately, midsized business IT departments typically have far fewer resources to bring to the problem than their larger counterparts. Compounding the problem, midsized businesses increasingly face the same distributed data protection challenges that plague larger companies. As branch offices proliferate and employees spend more and more time on the road, more and more data is being generated away from a company's mainsite. Lacking the resources to solve the problem in house, many midsized businesses are turning to a completely different kind of solution: remote on demand data protection services.

Under resourced and at risk

Being smaller doesn't save a healthcare company or brokerage firm from having its data retention policies audited by regulators. Litigation can happen to anyone. Earthquakes, blackouts and hurricanes don't discriminate between small and large companies or between a corporate data centre and a one-floor branch office.

Highlights

Local backups do not protect against any loss that happens outside the data centre.

Local disasters can destroy both primary data and onsite backups.

The costs of inadequate data protection are high. When unprotected data is lost, it often must be re-created from scratch. If a company is relying on local tape backups, any loss that happens outside the data centre is out of the IT manager's control. The problem is likely to worsen over the next few years as midsize businesses expand and the number of remote and branch offices increases. Factors driving this trend include offshoring of business processes, supply chain integration, expansion into key regions for competitive purposes, mergers and acquisitions and market globalisation. Branch offices often lack adequate onsite IT support. With limited resources to focus on backup and recovery, properly managing and protecting data can be difficult.

Tape backup: popular and problematic

Most midsize businesses use tape backup as their primary mode of data protection. However, this approach is unsatisfactory because it tends to be:

- *Unreliable and haphazard, posing the risk of being found non-compliant with federal, state, securities and business continuance mandates for companies of all sizes.*
- *Difficult to centrally manage, as IT staff 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 IT resource intensive, requiring servers, tapes, disk drives and backup software at every site.*
- *Slow and cumbersome, hindering the realisation 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.*

Highlights

The inadequacies of tape leave a company vulnerable to potentially serious costs.

Companies need to protect the information that is being generated remotely.

The inadequacies of tape leave a company vulnerable to potentially serious financial and business costs resulting from lost data, lost user productivity and regulatory fines.

Some companies have begun to replicate data back to the main corporate site, where it can be stored on disk and centrally managed. 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 (W A N) and local area network (LAN) bandwidth, potentially interfering with business-critical transmissions and end-user productivity.

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 IT 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 non technical end users.

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

Highlights

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

A better alternative

Many midsize business IT managers now realise that their current distributed data protection setup is inadequate, but they lack the resources to deploy and manage a more effective solution in house.

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

Midsize businesses can benefit from an on demand service solution through potential cost savings and ROI, high service levels and enhanced continuity, as well as service that can grow with a company's needs.

Potential cost savings and 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 physical facilities for offsite storage of backed up data.*
- *Labour 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 IT and end-user productivity, lost revenue and client goodwill, and regulatory fines).*

Highlights

Equipment, software and technical support are provided as part of the service.

A company does not need to be large to benefit from using a data protection service.

The right service provider can offer a level of distributed data protection that few midsize businesses can afford on their own.

Equipment, software and technical support are provided as part of the service, helping save the client on both capital and labour costs. Backup and recovery services typically run over a client's existing high-speed Internet connections. The client pays a monthly fee based on the volume of data protected.

A pay-for-service model not only helps save on capital costs, but also may allow a company to predict and plan for future expenses with greater ease and accuracy.

A company does not need to be large to realise potentially significant gains from using a data protection service. Midsize companies that turn their backup operations over to a service provider can save on labour time and reduce the downtime required to shut down the company's server and swap out a removable disk.

High service levels, enhanced continuity

What is most important is that the right service provider can offer a level of distributed data protection that few midsize businesses can afford on their own. IT managers can rest easier if they feel that backups will take place on schedule across all branch offices and designated PCs and servers and that RPOs and RTOs will be addressed.

A data protection service can also include around-the-clock support and monitoring, which most midsize businesses cannot afford but often need as their operations become increasingly global. Backed up data can be housed in the service provider's remote disaster recovery facility, increasing business continuity if a disaster should take out a client's branch office or even headquarters.

Highlights

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

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

Growing with a company's needs

For most corporate IT staff, keeping up with a company's growing data protection demands is a constant struggle as well as a major expense. Scalability is particularly important to midsize companies, which tend to expand in rapid spurts both organisationally and in terms of data capacity.

On demand services have the built-in redundancy, capacity and flexibility to help address the needs of companies of virtually 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 overutilised. As a further benefit, the on demand model helps IT administrators predict and plan for future costs far more accurately.

Established solutions demonstrate the efficacy of the on demand model

One such managed on demand data protection solution is IBM Information Protection Services – remote data protection service. This service helps companies protect data on servers, PCs and laptops across the organisation and from nearly any location. Data is automatically backed up via the client's existing network to our security-rich offsite data centres.

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.

Highlights

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

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

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 organisation'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 – because clients only pay for the amount of data they back up.

Benefits of the remote data protection service include:

- **Increased potential for cost savings and ROI.** *Equipment and support are provided for clients at disaster-resistant data centres, 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 utilisation is improved. And because critical data protection operations are automated, clients can redeploy personnel to other projects and significantly 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.*
- **Non intrusive, 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 client's changing needs as the amount of their data grows.*

Highlights

With on demand solutions, protecting and accessing data can be extremely efficient.

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

- **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 helps clients define specific, time-based data retention policies that better 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 feature 128-bit Advanced Encryption Standard (AES) encryption, which tends to be more secure because it helps ensure that only authorised users can access data. In addition, our disaster-resistant centres are designed to protect client data from even the most extreme natural events, which is one of the safest alternatives. The remote data protection service also features Statement on Auditing Standards 70 (SAS 70) Type II certification, which is important in helping ensure that backups will address both business and compliance requirements.*
- **Comprehensive platform support.** *The remote data protection service features powerful platform support for Microsoft® Windows®, UNIX® and Linux® operating systems, 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.

Capabilities and options for server 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 RapidProtect option for servers

Remote data protection RapidProtect is an onsite, security-rich data protection option for large enterprise branch offices or midsize businesses 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 RapidRecover option for servers

Remote data protection RapidRecover is a security-rich disaster recovery option for large enterprise branch offices or midsize businesses. 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.

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

Highlights

Data is automatically backed up on a daily basis.

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 midsize businesses.

Data from a client's desktop or laptop 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 IT 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

Midsized businesses need to re-evaluate the wisdom of protecting branch office and PC data with tape backups and other localized, do-it-yourself solutions. The risks and potential costs – of losing crucial information for good, interrupting operations, losing clients and being found noncompliant by federal regulators – are too great. And the price of failure 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 midsized businesses with reasonably priced distributed data protection.

For more information

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

ibm.com/au/bcrs

© Copyright IBM Australia Limited 2008.
ABN 79 000 024 733.

© Copyright IBM New Zealand Limited 2008.

© Copyright IBM Corporation 2008.
All rights reserved.

IBM Australia Limited
Level 13
601 Pacific Highway
St Leonards NSW 2065

IBM New Zealand Limited
171 Featherston St
Wellington

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

M35001