WHITE PAPER

Solving the Distributed Data Problem: The Rise of Remote Data Protection Services

Companies need to re-evaluate 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 non-compliance 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 an affordable, 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 customers. This is an ideal time to check them out.

WHITE PAPER

Solving the Distributed Data Problem: The Rise of Remote Data Protection Services

ARSENAL DIGITAL SOLUTIONS™

Executive Summary

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 and careless employees. Recent 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 multi-million dollar fines; not to mention serious losses in revenue, customer good will, market position, credibility, productivity.

Savvy corporate decision-makers have recognized that in order to deal with these challenges, they need to deploy a companywide, data protection infrastructure. However, doing it 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 IT control: at branch offices, 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.

This paper will first discuss the challenges that corporate IT managers face as they struggle to protect distributed data; and then go into how, on-demand data protection services enable companies to address those challenges reliably, securely and far more-cost effectively than a comparable in-house solution.

The Challenge

Businesses are responsible for protecting and securing an already extensive and rapidly growing body of information.

IDC predicts that by 2010, public and private organizations will be responsible for the security, privacy, reliability, and compliance of at least 85% of all information in electronic form of any kind (including MP3 files, photos, graphics, applications, etc.)

Managing and protecting that data has been become a major challenge for IT departments, primarily because most of it is being generated outside the corporate data center. More than 80% of employees currently work outside of corporate headquarters, according to Nemertes research.

Protecting data across a distributed enterprise constitutes a huge and growing IT expense. Nor can companies afford to put the problem on the back burner: the dangers and potential costs are much too high.

Explosive Data Growth, Increased Risk

- Managing and protecting data has become a major challenge for IT departments, primarily because most of it is being created outside firms' main corporate sites.
  "More than 80% of employees currently work outside of corporate headquarters"
  -- Nemertes Research
- Protecting data across a distributed enterprise with branch offices and a mobile workforce constitutes a huge and growing IT expense.
- Failure to retain critical information in a safe, secure, easily recoverable form has resulted in multi-million dollar fines for many companies.
- IDC predicts that by 2010, public and private organizations will be responsible for the security, privacy, reliability and compliance of at least 85% of all information in electronic form.

A recent Computerworld survey of IT professionals found that of those who reported data loss in the previous six months, 50 percent said the data was lost from desktops, and 24 percent said the loss was from remote branch offices.

The problem is only going to get worse over the next few years, for companies of all sizes. Medium-sized firms have an average of eight remote or branch locations, while large firms average sixty-five, according to IDC. Enterprises are likely to have more than one data center and main office, particularly if they have overseas operations. IDC expects the number of branch offices to continue expanding over the next five years.

Factors driving this trend include off shoring of business processes, supply chain integration, expanding into a key region for competitive purposes, mergers and acquisitions, and market globalization.

Smaller companies tend to have few or no branch offices; however, their IT staffs generally consist of one or two people who are solely responsible for the entire computing operation. As a result, their headquarters sites often have even less technical resources to devote to backup and recovery than a typical enterprise branch office.

Tape Back Up: Popular and Problematic

For sites with little or no local IT support, tape backup is has become the de facto data protection strategy. However, this approach is unsatisfactory for several reasons:

Tape backups tend to be unreliable. Enterprise Strategy Group estimates that 60% of traditional tape back ups fail. Moreover, with no on-site IT support at many branch offices, data protection becomes the responsibility of overworked office administrators and business users who lack the time and willingness to follow corporate backup schedules and procedures. And central IT staffs have no way to monitor remote operations in order to ensure that backups take place, and are successful.

Security is another major issue: unencrypted tapes are a tempting target for thieves. And they are easily lost or stolen, particularly in transit: for example, when they are being moved to a secure off-site facility.

Trouble With Tape

- Most SMBs use tape backup as their primary mode of data protection.
- Out of all the smaller companies that responded to a recent Gartner survey, 59% said that they only do local back up - which means that if a company's data center or branch office is destroyed by a disaster, the company loses both primary and backed-up data.
- "Disaster recovery and restart could take days, even weeks, because you must know exactly which tapes you need, locate them, retrieve them, import them into your library, and restore them."
  -- Forrester Research

And while the tape media itself is inexpensive, setting up distributed tape backup on multiple sites can be costly. Companies must pay for redundant equipment and software across all sites, and lose the cost advantages of volume discounts and centralized bargaining with vendors. As branch offices proliferate and data volumes keep growing, companies keep having to add more tape drives. Furthermore, each site tends to choose its own equipment and software.

Centrally managing tape backup across these incompatible solution islands is also extremely difficult. With many branch offices lacking on-site IT support, backup responsibilities tend to fall on an overburdened office administrator or a business "power user," who tends to put such tasks at the bottom of his or her to do list. As a result, backups are performed irregularly at best, and IT gets called in whenever a system problem develops. To make matters worse, IT administrators have no monitoring system to tell them whether a backup was performed, or successful.

Meeting Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) is also problematic, even when tape back ups are regularly performed: "Disaster recovery and restart could take days, even weeks, because you must know exactly which tapes you need, locate them, retrieve them, import them into your library, and restore them," a 2006 Forrester report states.
Which leads us to the biggest potential expense of using tape backup: the potential financial and

business costs of lost data, lost user productivity, regulatory fines, that result from inadequate data protection.

As a result of these realities, tape back up is an unsatisfactory distributed data protection solution because it tends to be:

- Capital and IT resource intensive, requiring servers, tapes, disk drives, and backup software at every site
- Labor intensive, often interfering with the regular jobs of on-site employees
- Unreliable and haphazard, posing the risk of being found in non-compliance with federal, state, securities and business continuance mandates for companies of all sizes
- Slow and cumbersome, hindering the realization of RPOs and RTOs
- Most importantly, leaves a company vulnerable to serious data loss

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 repalication software. Network costs increase as well, since periodic server backups tend to hog WAN and 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 the corporate headquarters and IT control. Protecting and securing this critical and sensitive information, which includes customer records and intellectual property, becomes the sole responsibility of these time-challenged and often non-technical end users.

The need to protect such devices is urgent: at least 15% of all laptops are stolen or suffer hard disk failures. 31% of all PC users have lost all of their files due to events beyond their control. Furthermore, 10% of PCs are infected with viruses every month, with over a third of these infections resulting in data loss.

While remote PC backup products are available, they tend to be bandwidth- and CPU intensive, slowing down application and network response time, annoying users and negatively impacting productivity.

A Viable Alternative

The situation outlined above poses a serious dilemma for many corporate IT departments. They realize that their current distributed data protection set up is inadequate, and that a centralized infrastructure is the best way to go, but lack the resources to deploy and manage it in-house.

Fortunately, there is a better way to go: an on-demand distributed data protection service that automatically backs up off-site PCs and servers, automatically, reliably, securely, anywhere on a customer's IP network.

On-demand data protection services are fully turnkey solutions that provide hardware and software, centralized management and reporting, 24/7 monitoring and management, third party hosting, and off site Tier 1 data facilities. Remote, on-demand services have become the data protection solution of choice for a growing number of companies of all sizes. According to a recent survey by TheInfoPro, nearly 20% of Fortune 1000 organizations outsource at least some portion of their storage management activities. About one-third of companies surveyed had outsourced day-to-day backup activities. Over 15% outsource their disaster recovery sites, cable plants and day-to-day break/fix storage activities.

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

Evaluating ROI

When evaluating return on investment for a service-based protection solution, a company needs to take into account all of relevant cost factors 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 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. These include, but are by no means limited to: loss of IT and end user productivity, lost revenue and customer good will and regulatory fines.

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

Companies that have turned over their data protection operations to an on-demand service have reduced business continuity expenditures by more than 80%, and lowered IT capital expenditures by more than 20%, according to IDC.

High service levels, assured continuity

Most importantly, the right service provider guards against the high costs of data loss, by providing a level of distributed data protection that most companies cannot afford on their own. IT managers can rest easy knowing that backups will take place on schedule across all branch offices and designated PCs and servers; and that RPOs an RTOs will be met. Data can be housed in the service provider's remote disaster recovery facility, ensuring 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 and a major expense as well. On-demand services have the built-in redundancy, capacity, and flexibility to meet the needs of any sized company, and to scale up – or down – quickly and seamlessly 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 over utilized. As a further benefit, the on-demand model enables IT administrators to predict and plan for future costs far more accurately.

Established solutions demonstrate efficacy of the on-demand model

One such on-demand data protection solution is ViaRemote®, a fully-managed, on-demand data protection service from Arsenal Digital Solutions.

This offering enables companies to protect data from all servers, PCs and laptops across the organization, no matter where they are located. Data is automatically backed up via the customer's existing network to the provider's secure, off-site data centers.

ViaRemote is a pay-for-usage subscription service, making data protection costs highly predictable and affordable for its customers. The service includes all the hardware, software, and operational support needed to quickly and easily implement a best practice based data protection strategy. This unique approach eliminates the research, implementation, hiring, and training costs of launching an in-house solution – while accelerating service delivery.

Data is backed up automatically on a daily basis, delivering extremely fast performance with minimal demand on customers' networks. This provides a fast, cost-efficient and convenient way to provide consistent data protection across all of an organization's servers, PCs and locations, without the need to increase network investment.

The service is cost-effective for any size business — from large, global enterprises with multiple sites to small and mid-sized businesses - because customers only pay for the amount of data they back up.

Benefits of on-demand services such as ViaRemote include:

Increased cost savings and ROI. All equipment and support is provided for customers at disaster-proof data centers, reducing the need for capital investments in hardware or software. Pricing is based on the amount of data customers protect, enabling them to control their costs because capacity utilization is constantly optimized. And because critical data protection operations are automated, customers can redeploy personnel to other projects and significantly lower their backup and recovery management costs.

Effortless offsite data protection. On-demand solutions provide reliable, efficient, automated off-site daily backups of server and PC data for business continuity and disaster recovery, regardless of where the data resides (branch offices, mobile workforce, etc.).

Higher service levels and assured continuity. Backup and recovery of vital business data is supported and managed 24 hours a day, 365 days a year.

Non-intrusive, scalable backups. Advanced technology minimizes the bandwidth required to protect customer data, ensuring optimal computer and network performance. High-capacity infrastructure enables providers to meet customers' changing needs as data grows.

Ease of use. Intuitive applications and web portal interfaces make it easy 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 on-demand solutions such as ViaRemote, protecting and accessing data is extremely efficient.

Flexible retention policies and long-term archiving. Services like ViaRemote allow customers to define specific, time-based data retention policies that match their business needs - from dailies, weeklies, and monthlies to yearly retention options for compliance. And the best solutions also provide the option to archive everything to tape for long-term retention.

Security and compliance. Services that feature128-bit AES encryption are the most secure, because they ensure that only authorized users can access data. In addition, Tier 1, disaster-proof centers that protect customer data from even the most extreme natural events are the safest alternative. SAS 70 Type II certification is also important to ensure that backups will meet both business and compliance requirements.

Comprehensive platform support. Services that feature powerful platform support to include Windows®, UNIX, and Linux operating systems and leading databases such as Oracle and Microsoft Exchange and SQL offer the ideal capability for most businesses.

Arsenal's ViaRemote service offers a number of interesting capabilities and options specifically for server data protection:

Onsite Appliance Option for Server Data Protection

The ViaRemote Appliance option provides rapid onsite data recovery to help meet increasingly stringent recovery time objectives (RTO). This service is delivered through installation of a preconfigured storage appliance on the customer's local area network, enabling a failed server to be recovered in hours rather than days.

Bare Metal Recovery Option for Servers

The ViaRemote Bare Metal Recovery option is a fully-managed and automated solution that enables customers to rapidly complete a "bare metal" recovery of their server operating system and applications up to 80% faster than traditional methods. With this service, customers have the most reliable and cost-effective tools available for bringing their business back online quickly.

ViaRemote RapidProtect Option for Servers

ViaRemote RapidProtect is an on-site, secure data protection option for large enterprise branch offices or small to mid-sized businesses that dramatically reduces 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 then imported. Once the data is on Arsenal's service platform, incremental backups completed over the Internet are performed in a fraction of the time typically required.

ViaRemote RapidRecover Option for Servers

ViaRemote RapidRecover is a secure disaster recovery option for large enterprise branch offices or small to mid-sized businesses. In the event of a server or site disaster, an appliance with all customer data is quick-shipped to the customer's D/R or original location to reduce recovery time. Large server restore time is greatly reduced by eliminating the need for large restores to be sent across the Internet.

For desktop and laptop PC data protection, Arsenal's ViaRemote service offers a fully-managed online data backup and recovery service that meets all critical data protection, business continuity, and financial requirements for both large enterprises and small to mid-sized businesses.

Data from all of a customer's desktops and laptops, wherever they are located, is automatically backed up on a daily basis through the customer's existing network connection to a secure offsite storage facility. All mission critical data is centrally managed, securely protected, and easily recoverable, whenever it is needed.

Operationally, ViaRemote is a fast and highly efficient solution. By transmitting only data that has changed since the last backup, ViaRemote minimizes the bandwidth required to perform these operations. This ensures that individual computer and network performance is not impacted, and allows customers' staff to continue working during the backup process. Data can easily be backed up and restored by individual users at any time, without any IT support, using the intuitive ViaRemote user interface. Users log into the application, and simply select the data they would like to backup or restore. With the ability to select single files or entire folders, users can retrieve different versions of their files from any backup performed during the last 30 days.

Conclusion

Companies need to re-evaluate 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 non-compliance 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 an affordable, 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 customers. This is an ideal time to check them out.

This paper is brought to you by Arsenal Digital Solutions.

About Arsenal Digital Solutions

Arsenal Digital is the worldwide leader in on-demand data protection. We offer a comprehensive suite of award-winning services for server and PC data protection, backup and recovery, business continuity, disaster recovery and regulatory compliance.

With nearly a decade of experience and an unparalleled technology and service infrastructure, we are uniquely qualified to meet the needs of companies of all sizes in today's challenging distributed data environment. We serve thousands of customers globally from Fortune 50 companies to emerging businesses, and we are the data protection partner of choice to many of the world's top network service providers, OEMs, and ISVs.

Our rapidly growing customer data footprint currently exceeds 20 petabytes (PB), proof that we are overturning the industry's traditional purchased hardware/software approach with a proven, flexible, on-demand service that sets a new benchmark for automation, reliability and scalability.
For more information about Arsenal, our services and solutions, visit www.arsenaldigital.com or call 919-466-6700.