keymethods

WHITE PAPER

SMBs Need More Than Just Backup (but they don't need to spend more)

Top 5 Criteria for Choosing the Right Solution that Protects Your Data and Keeps Your Business Up and Running

Introduction

Small and medium businesses (SMBs) need to keep their businesses up and running just as much as larger companies. Yet they are challenged by several limitations when seeking out a solution that meets their mission-critical data recovery, application uptime, and data retention needs. These include:

- Limited funds
- Limited IT resources
- Limited/inadequate solution options designed for SMBs

With these challenges in mind, this paper identifies and explores the top 5 evaluation criteria SMBs should carefully consider when determining the best solution for their data protection and business continuity requirements. SMB end users should feel confident in implementing a solution that they find meets all of these criteria.

Top 5 Evaluation Criteria for SMB Data Protection and Business Continuity Solutions

1. Recoverability: How quickly and completely does the solution deliver data recovery and server recovery? Does it meet both recovery time objectives and recovery point objectives?
2. Comprehensiveness: Does the solution offer a complete, integrated range of data protection, business continuity (data, application or server continuity), disaster recovery, and archiving services?
3. Ease of Use: Does the solution provide non-disruptive deployment, management (set it and forget it), and ongoing operation (simple recovery and failover/failback)?
4. SMB-specific Focus: Is the solution truly designed for SMBs? Or is it an unwieldy and expensive retrofit of a solution meant for large enterprises or an under-featured consumer solution being sold to SMBs? Does the solution offer business-class functionality in a form factor that meets the simplicity and ease of use requirements of SMBs? Does the vendor have a user base of small and medium businesses?
5. Affordability: Is the solution cost-effective to implement from day one and over the long term? Does it offer a pay-as-you-grow approach?

Criterion #1: Recoverability

No evaluation criterion is more important than data recoverability. Unfortunately, determining the true recovery capabilities of an SMB backup solution can be a daunting undertaking. Potential customers should ask a vendor questions about the scope of data recovery (e.g. does the solution recover entire applications or just files?), the speed of recovery (known as the Recovery Time Objective or "RTO") and the amount of potential data that can be lost before protection kicks in (known as the Recovery Point Objective or "RPO").

How automated are the recovery processes of the given solution? Do they require a detailed human intervention to initiate the recovery process and restore the data or do they recover automatically? What kinds of management controls will the IT user possess over setting recovery controls? Does the solution have complete and consistent recovery capabilities for all applications or just a subset? These are some of the top questions to which every customer should expect detailed, consistent answers from their vendors.

Criterion #2: Comprehensiveness

It is a fact of technology life that data protection and business continuity always require a number of "moving parts" (e.g., applications, servers, networks, storage, and human-driven policies), but not all vendors have done an equal job assembling those moving parts into a seamless whole. For example, it is well known that many SMBs find themselves managing entirely separate backup and replication products and policies in order to support different infrastructure and protection goals. There is a hidden cost to this complexity that exposes the organization to data protection risks and inefficiencies. Given the complexities of SMB IT management today, this kind of approach will not stand the test of time and growth.

The alternative: SMB IT teams should look for data protection and business continuity offerings that integrate key functionality into a unified offering. The integration of these capabilities reduces the costs associated with management, growth, support, and data recovery. Simplification through comprehensive coverage should be a key goal for SMB data protection purchasing.

Online backup is a step in the right direction, and it's a good start in the evolution of backup from the outdated tape model to a disk-to-disk model of data protection. However, online backup is a piece of the puzzle and not an overall solution. For a total data protection solution you need a combination of on-premise and cloud-based services.

Criterion #3: Ease of Use

Many data protection offerings will claim that they are "easy to use," but the proof is in the details. Ease of use should be measured not just in the obvious areas of the user interface at initial deployment and integration, but in ongoing management, scaling, and most importantly, at the time of data recovery. SMB IT teams should make sure that any potential offering is put through its paces across all of these areas. It is important to ask questions about how the solution will integrate with the application, server and storage environment, and its ability to support specific and automated recovery policies.

Criterion #4: SMB-specific Focus

The history of the backup industry is littered with large company technologies that failed to answer the unique requirements of the SMB world. The reason is simple: it is impossible to make large enterprise backup and business continuity products seamlessly meet the requirements of the SMBs. When evaluating offerings, make sure that the vendor truly understands and serves the SMB market. Are their customers like you? Can they prove it? Does their technology seem purpose-built to satisfy the human, financial and technology challenges of the SMB IT world? Does their support infrastructure adequately reflect a focus on the SMB customer, as well? All of these elements are critical to ensuring successful deployment and management of an SMB data protection solution. Sometimes, the large company name and logo, while trustworthy, leads to a false sense of security as many enterprise vendors do not pay attention to the unique needs of SMBs. This often results in the purchase of a poorly suited data protection and business continuity purchase.

Criterion #5: Affordability

The initial cost of a data protection or business continuity solution accounts for only a part of the true cost of a comprehensive solution. The true costs of deploying and scaling a data protection environment show up in the costs of human management, technical support, and flexibility (or lack of flexibility) experienced when growing the infrastructure. Many backup offerings entice customers with a low advertised fee— only to surprise them, once they've dedicated time and resources to using the solution, with unplanned management costs, license costs, costs for plug-ins, and other hidden costs. Others require a significant to massive capital expenditure upfront, so that customers are forced to guesstimate their companies' future growth and pay for more services and storage space than they actually need.

The keys to avoiding the price trap of the SMB backup world are to look for transparency and simplicity in the pricing model. There is no rule that says backup pricing should be complex! Further, your initial investment should be flexible to meet your current needs, but should be able to scale proportionally and provide you long-term gains as you grow, not the other way around. The best practice is to work with vendors and their partners who provide simple, transparent pricing; integrated services without hidden fees; and a low Capex, pay-as-you-grow model that scales in a way that saves you more money in the long run because you are not paying for services you are not using.

A Comparison of Data Protection Methods

The traditional and most widely deployed data backup methodology is tape—companies store daily, weekly and monthly point-in-time copies of data to a tape media for short term and long term, offsite storage. In recent years it has become increasingly well understood that tape is an unreliable, ineffective form of backup with numerous hidden costs. Tape cartridges can break down over time, are a continuing cost for already strained IT budgets and completing daily tape backups requires significant attention from IT administrators. Moreover, recovering data from tape is a cumbersome process as an entire backup needs to be located amidst the collection of tapes and restored in order to restore just a file or set of files.

Some companies today offer online-only backup services that utilize agent-based software (installed on every device) to send backup data offsite via the Internet for data protection. Although online backup sounds easy, the primary limitations of this method are that it fully depends on Internet connections for transmission of data. As a result, backing up data takes an extremely long time, and companies are often forced to wait days or even weeks to restore data that is larger than just a few small files.

Recently companies have begun to offer backup via software as a service solutions that provide a managed service provider form of backup.

The ideal data backup solution for SMBs is a hybrid onsite/offsite or cloud backup solution that deploys an appliance with local storage at a company's office but also leverages the internet to provide online backup as well. The appliance is able to store the local backup and then replicate that data across the Internet to cloud storage. With this solution, performance impact is minimized and data restore issues can be done much faster. In addition, with data backup occurring both on-and offsite, multiple copies of data backup exist to ensure total data protection and recovery.

How Key Methods Backup & Disaster Recovery Server (BDR) Meets the Top 5 Evaluation Criteria for SMB Data Protection and Business Continuity Solutions

Key Methods BDR offers the first data protection service to make business continuity and online backup

simple for small and medium businesses (SMBs) by delivering a secure and cost-effective way to ensure uptime and data recovery.

Criterion #1: Recoverability

How quickly and completely does the solution deliver data recovery and server recovery? Does it meet both recovery time objectives and recovery point objectives?

With our Backup & Disaster Recovery Server (BDR), SMBs are protected in two ways: there is a device that stays at the customer site and stores the company's data and server images, plus a copy is stored remotely by Key Methods in a secure, offsite location. This means multiple copies always exist, ensuring that the business is protected no matter what. If something unfortunate happens – such as a server crash, accidental deletion, hard drive or file corruption, computer virus, laptop theft, phishing attack, keyboard spill the company is just a mouse click away from recovery.

The BDR suite of self-managing data protection services preserves application availability even if a server fails and it restores lost data quickly, enabling SMBs to meet or exceed their recovery time objectives (RTO). Our BDR onsite data protection device allows lost data to be restored in minutes, not days, weeks or even months like other solutions. This is different from online-only backup vendors, who are unable to deliver recovery speed when you need it most. Why? Because the only copy they store of a company's data resides offsite, meaning that the rate at which they can send it back is limited by both Internet bandwidth and the distance the data needs to travel. With the BDR, SMBs can back up data automatically or manually at frequent intervals – hourly if needed, with little or no impact on server performance.

For a total data protection solution, IDC analyst Ben Woo has stipulated that SMBs need a combination of on-premise and cloud-based services – and that is precisely what the BDR's unique model delivers for SMBs.

Examples of Real-world Data and System Recovery

Recovery Problem	Industry	BDR Solution
Server Failure 80GBs of critical financial data had to be restored from tape. Took over 3-4 weeks with limited success	Construction Firm	When the financial server crashed again, the BDR's disk to disk hybrid solution allowed the reseller to replace the server and restore data from the BDR's local appliance in about 4 hours without losing any data
Data Corruption Exchange database of 60GBs of data was corrupted over a weekend	Software Company	Utilizing the BDR to store the data at LAN speeds, the reseller was able to restore the database remotely in 2 hours
File Deletion Lead architect accidentally deleted a crucial file 30 minutes before a presentation for multimillion dollar deal	Architecture Firm	With the Key Methods BDR, the company was able to retrieve the file in 5 minutes and the company got the deal
File Deletion Disgruntled ex-employee ran a "delete c:*.*" on their trading server	Commodities brokerage Firm	BDR allowed them to be up and running within 2 days (data center burn to disk and ship)
Hardware Theft Server was stolen	Catering Company	After new hardware was purchased, all data was restored quickly
Hardware Theft CEOs laptop was stolen	Accounting Firm	Company had a spare laptop in inventory and was able to fully recover all of the CEO's data in a matter of hours

Criterion #2: Comprehensiveness

Does the solution offer a complete, integrated range of data protection, business continuity (server failover), disaster recovery, and archiving services?

Key Methods BDR is a total data protection solution that delivers the best of an on-premise solution and the best of a cloud-based solution all as a single, integrated service. It is the one solution on the market today that provides a unified business continuity and data protection platform exclusively for SMBs with all of the necessary components built into an agentless platform:

- Encrypted backup of servers, workstations, and laptops for 360 degree data protection with rapid recovery
- Disaster recovery from online backup to an offsite location
- Archiving
- Server failover for business continuity (available 2H 09)

The Backup & Disaster Recovery Server offers all the services that SMB customers demand for backup, business continuity, disaster recovery, and long term data retention:

BDR RapidRestore™ Data Backup Services

- Desktop, laptop, and server backup
- Fast, network-speed restores from the BDR appliance that allows RTO to be met
- Supports restore of a whole volume to its original location or, with Advanced Restore, selection of a version of a file or folder to restore it to a chosen location
- Support for multiple concurrent operating systems, including Windows, Linux and Mac OSX
- Built-in integration with popular applications such as Microsoft Exchange and Microsoft SQL Server
- Open file and active directory backup

BDR SmartDR™ Disaster Recovery Services

- Data and system protection for rapid return to business in the event of a site failure
- Customer data is stored in multiple offsite locations fitted with the latest security measures to protect data from fire and theft
- In the event of a site failure, a new BDR appliance, fully loaded with business data and system information, is shipped to the company's new or temporary location as soon as it is needed.

BDR SmartArchive™ Data Retention Services

- Flexible scheduling for long-term online data retention
- AutoVersioning capability for point-in-time restore enables RPO to be met

BDR ServerAlive™ Server Continuity Services

- Bare metal backup and restore functionality offers quick, one-click restore of a server image to new hardware. Makes it easy to restore the operating system, applications, and data onto new hardware without having to install operating system, settings, and applications, etc.
- An image of each protected server is kept on the BDR data protection appliance. If the original server dies, a company can boot off of the server image and work off of that until the new server hardware arrives.
- This feature can be activated on the specific servers that a company chooses to protect

Criterion #3: Ease of Use

Does the solution provide non-disruptive deployment, management (set it and forget it), and ongoing operation (simple recovery and failover/failback)?

Key Methods BDR is extremely simple to deploy and manage:

- No disruption to the SMB IT environment
- No limitation on how many servers, workstations or laptops can be protected
- No lost data, no downtime
- Simple pricing - no hardware or licenses to purchase
- Automated data recovery and server continuity

By virtue of being agentless – i.e., there is no software installed onto servers and workstations – the majority of the computing is done on the BDR onsite device, eliminating impact to the business environment. One of the major complaints about the agent-based solutions on the market today is that they consume significant computing power on the machines on which the business is supposed to be running, slowing down performance from the end users' perspectives. This is simply not an issue with the BDR.

Criterion #4: SMB-specific Focus

Is the solution truly designed for SMBs, or is it a retrofit of enterprise solutions or an underfeatured consumer product masquerading as an SMB solution? Does the solution offer enterprise-class functionality in a form factor that meets the simplicity and ease of use requirements of SMBs? Does the vendor have a user base of small and medium businesses?

The Key Methods BDR solution is purpose-built from the ground up to serve the needs of small or medium sized businesses managing anywhere from 1 to 500 workstations or servers and 10GB to 10TB+ of data. Businesses across a wide range of industries including legal, financial services, healthcare, design and creative industries (engineering, architecture, graphic design, etc.), retail, credit card services, webbased companies and education currently use the BDR to protect their data and keep their businesses up and running.

Many SMBs have a combination of operating systems across the laptops, servers, and workstations in their organization. This may be by design, for example because graphic artists in a company use Mac systems, while sales and other functions use PCs. Or it may be an unintentional fact of life, because two organizations have joined to create the business or because employees in a young company are using their own disparate machines. Whatever the reason, Key Methods provides a solution that doesn't force the SMB to deploy several different data protection schemes. Unlike many SMB solutions that will not work with a combination of operating systems or favor one platform over another, The Backup & Disaster Recovery Server is fully compatible with multiple concurrent operating systems. Whether an SMB has Windows machines, Macs, Linux, or a combination thereof, their entire fleet of workstations and servers can be reliably protected by one simple solution.

Criterion #5: Affordability

Is the solution cost-effective to implement from day one and over the long term? Does it offer a pay-as-you-grow approach?

The loss of one week's worth of data produced by one individual in an SMB organization is more costly than paying for the BDR for an entire year.

Key Methods BDR cost benefits entail:

- No upfront costs
- No cost for multiple licenses
- No hidden costs
- Pay-as-you-grow model
- Comprehensive, integrated solution from one provider

Conclusion

Can your company afford to lose 23 hours of data? What about 12 hours? Small and medium businesses today require a data backup solution that fits the specific needs, IT infrastructure and budget of their company. In order to choose the right solution, IT administrators should use the top five criteria for SMB data protection solutions including: data recoverability, solution comprehensiveness, ease of use, SMB-specific focus, and affordability.

With an easy to use, flexible solution, Key Methods has developed a hybrid onsite and cloud data protection and business continuity solution that enables backups to be scheduled as often as needed with little to no impact on server performance and gives IT administrators the ability to restore data as quickly as possible and ensure uptime and data recovery throughout the organization.