The New Case for Continuous Data Protection: Challenges, Best Practices and Solutions

Best practices for SMBs to attain complete data and application recovery.

CONTENTS

SONICWALL®

Abstract:
This paper examines the challenges faced by small and mid-sized businesses (SMBs) in their attempt to attain complete data and application recovery, reviews best practices to overcome these challenges, and explores how best practices can be met using SonicWALL Continuous Data Protection (CDP) Series solutions.

Backup and Recovery Challenges

Any backup is only as reliable as its ability to restore business data and applications when they are needed most. Small and mid-size businesses (SMBs) today are challenged not only with complex, burdensome backups, but just as importantly, with unreliable and incomplete data recovery. While conventional batch-process tape-based backup hasn't changed significantly in over 30 years, it remains the approach that most SMBs still use to protect their computing environments.

Increased complexity and burden on SMBs

Data backup has become more complex and burdensome. In attempting to deploy a complete backup and recovery solution, most SMBs end up juggling multiple software and hardware point solutions of varied quality that often require complex integration and support from multiple vendors.

At the same time, resources are tighter. More than ever, SMBs are struggling do to more with less. SMBs are challenged to find a single backup and recovery solution to do it all within the restraints of limited budgets and staffing resources. IT administrators often have multiple roles and responsibilities, and have less time to devote to ensuring their backups. Restorations are most commonly performed for a single file only. The administrative overhead in a tape based system to find the tape, find spare disk space, restore the entire file system, and extract each single file is relatively immense, and places an enormous burden on administrators.

Today data is more distributed across multiple physical sites and device types. The rise in mobile device usage alone poses its own unique issues for backup and recovery. Offsite unmanaged and personal computing devices can be especially vulnerable to data loss from viruses and other malware. IT is less able to enforce verbal or written backup policies with remote or mobile end-users. Laptops and other mobile devices are inherently subject to physical damage from being dropped onto hard surfaces. Increasingly, data on laptops and other mobile devices is lost due to theft.

Traditional backup policies are notoriously unreliable. Most SMBs rely on written or verbal polices that require users to manually save important documents to the network. End-users forget to save files, unintentionally delete important data, and accidentally damage their computer systems. SMBs are often left uncertain whether a viable backup has even occurred. Connections to servers and other computing devices may be compromised before or during backup for various reasons, without the administrator being aware. Since administrators often establish backups in the middle of the night to avoid impacting network performance, the backup will miss any laptops that were brought home or no longer connected.

Data recovery from conventional tape systems has been unreliable. According to one published survey[1], 77% of respondents found failed tapes while testing their backup system. Even though tape is widely recognized as unreliable, as many as three out of four SMBs still back up information using tape solutions. While hardware failure is the most common cause of lost data, human error accounts for a significant amount of data loss. Conventional tape backups require manual intervention, and are prone to inadvertent administrative errors.

[1] *Storage Magazine*

Limited capabilities of conventional solutions

SMBs have more at risk than just individual data files. Today, SMBs must protect increasingly expanding volumes of data and the application and server systems that support them. Mission-critical information is stored, tracked and organized across multiple server-based systems, not only in a single "backup" folder. Server-based applications such as Exchange, SQL Server and Active Directory present complex data ecosystems that must be backed up and recovered along with individual files. Transactional histories from applications that interface with customers or partners are crucial for reestablishing business operations. IT demands that all current logs, patches and configuration files are saved in order to rebuild systems after a disaster. Additionally, SMBs need to meet stricter regulations for long-term data archiving. SMBs are mandated to comply with emerging industry and government regulations such as the Payment Card Industry Data Security Standard (PCI) and the Health Insurance Portability and Accountability Act (HIPAA). E-discovery has become more commonplace in legal and tax auditing proceedings. Audit trails require multiple versions of broader types of data, as well as digital communications such as e-mail.

Conventional tape backups are limited in their capability to support application recovery because they produce a single-point-in-time copy of the application data stored on secondary storage media. The recovery process is divided into two parts, data restoration and application recovery. Data restoration consists of copying potentially valid data from one location to another. When basing their recovery on these copied images, SMBs must rely on the most recent uncorrupted image.

An SMB should not directly attempt to recover applications using a single-point-in-time image, because that image is the only preserved copy of the previous data image. Instead, the contents of the image should be copied to another location for recovery. If the image were to be corrupted during the recovery process, an SMB would be forced to use an older image, potentially resulting in more data loss. As a result, recovery time is dominated by data movement. There is nothing dynamic about single-point-in-time images, and they must be treated as very fragile.

Conventional tape rotation schedules often overwrite previous tapes. For example, in the commonly-used "grandfather-father-son" approach, an SMB earmarks a tape for each day of the week and rotates these tapes on a weekly basis, eventually overwriting earlier data. All daily file changes from the week before are lost. Depending on the weekly schedule, the fifth weekly rotation typically will overwrite the first. At this point, the most granular backup resolution is at the weekly level, except for the current week where dailies are available. Generally, at the end of the first month a monthly snapshot is taken. The limitation of this approach is the gap in the backup window (backup resolution). As tapes are overwritten, the ability to recover data to a specific point in time becomes more difficult. After two months, the best backup resolution will be at the previous month. After three weeks, the best resolution will be at the weekly level. (While an archive can be taken at any point in time, however, this is outside of the tape rotation process.) With conventional tape rotation, an SMB can only go back to the previous month's data. Any incremental changes made to a file between months will be lost.

Another critical limitation of conventional tape-based solutions is in speed-to-recovery. Restoration of crucial data can take hours, even days. Every minute wasted in getting core data and systems back up to business-as-usual can equate to lost revenues and greater competitive disadvantage.

Businesses are left unprepared

Ultimately, the complexity and limitations of conventional backup solutions mean that SMBs cannot depend on them for reliable disaster recovery. Additionally, many SMB recovery efforts are hampered by having backed up all of their information at a single site, presenting a single point of failure when that site is damaged or destroyed by natural disasters or other catastrophic events. Even where the backup media remains viable, SMBs can be limited in their disaster recovery efforts because the data or applications needs to be restored to hardware and operating system environments that are identically configured to the original devices, and there are no or few such devices available on hand at the recovery site.

Best Practices

To overcome these challenges and obstacles, administrators need to re-evaluate their backup and recovery approach, and apply effective, SMB-focused best practices when considering their alternatives.

Keep it simple

The ideal solution should provide a one-stop, integrated solution that is easy to deploy and manage, and not demand full-time support from IT staff resources. Administration of backup policy updates, enforcement and scheduling should be centralized and provide an easy-to-use, intuitive interface. Less complex solutions also tend to be more efficient and cost-effective.

Establish reliability through automation

SMBs should consider modern disk-based solutions that can provide fully-automated data and application protection. By automating data backup, SMBs can establish a foolproof process that no longer relies on the presumed actions or inactions of individual users or administrators. Automation enables administrators to reliably enforce policy-driven backups that are performed entirely transparently to end-users, helping to ensure that data, applications and systems are reliably protected from loss, potential disaster and malicious attack. Automation can facilitate data being backed-up as soon as it is created or changed, anytime the device is connected to the network. Automated solutions may also provide administrators with historical tracking and reporting, as well as generate alerts warning of any anomalies in scheduling or connectivity.

Provide immediate, granular recovery options

In a business emergency, recovery can't wait. A viable solution should provide the capacity and performance to quickly recover all mission-critical data and applications. Disk-based solutions can provide the capability to locate and recover information in minutes as opposed to hours or days. In order to comply with internal and external regulations, data should be securely encrypted and recoverable from multiple historical points in time. To enable complete restoration of business processes, a solution should be able to back up and recover the entire business system environment, including client-server applications, operating systems, databases and e-mail.

Empower users to securely recover individual files

Optimally, a solution should also enable simple user-based data and system restoration without demanding full time support from IT staff resources. Enabling secure self-directed restore capability can significantly and dramatically reduce the administrative burden for larger companies and frees up the system administrators for more productive work. For smaller companies that may not have the budget for in house system administrators, this alone can justify the deployment of a disk-based backup and recovery solution.

Build flexibility into disaster recovery plans

SMBs need the flexibility to immediately recover the most current data to new locations or computer platforms in an emergency, independent of single points of failure. A preferred solution would enable redundant backups to be duplicated securely over the Internet to separate business locations or a hardened data center, as well as archives to portable USB drive devices for offsite storage. In case the primary data site becomes unviable, administration and recovery must be supported remotely. Servers, desktops and laptop systems must be recoverable to their original environments if available or, if not, to differently-configured or virtual platforms.

The SonicWALL® CDP Solution

The SonicWALL® Continuous Data Protection (CDP) Series offers the only complete end-to-end, disk-based backup and recovery solution for SMBs. SonicWALL offers a wide range of CDP appliance models scaled to fit the budget, performance and capacity needs of any SMB. With capacity up to 9 TB at typical 2:1 compression, GbE connectivity, RAID 5 and replaceable components, CDP solutions are designed to meet today's demanding requirements for performance and reliability.

True low-touch administration

SonicWALL CDP takes the complexity out of safeguarding business data by automating tedious backup administrative tasks, providing an easy-to-manage, low-touch solution. CDP solutions ensure reliability and speed recovery by automatically generating e-mail alerts on any compromised connectivity and regularly-scheduled reports on backup activity.

Automatic, transparent and policy-driven solution

SonicWALL CDP delivers automatic, transparent backup that ensures data, applications and systems are reliably protected from common user error, hardware failure, deletion, potential disaster and malicious attack. By enforcing policy-based backup, CDP ensures control of all business critical data, while avoiding the increased costs of backing up non-business related files such as personal music, videos and pictures. Administrators can easily pre-configure set policies to ensure that specific business-critical files, folders or applications are backed up, and to assign end-users rights to allow them to retrieve their own data. An ideal replacement for tape-based systems, CDP solutions provides foolproof, intuitive continual protection.

Self-directed restore

SonicWALL CDP enables administrators to allow end-users to securely restore their own files. Self-directed restore increases user satisfaction and productivity while freeing IT resources.

Flexible disaster recovery options

SonicWALL CDP provides flexible backup and recovery options that enable SMBs to be up and running quickly after a disaster event, including Offsite Data Backup, Site-to-Site Data Backup and Local Archiving, as well as Bare Metal Recovery with Universal Restore of complete systems—OS, files, applications, databases and settings—in just minutes.

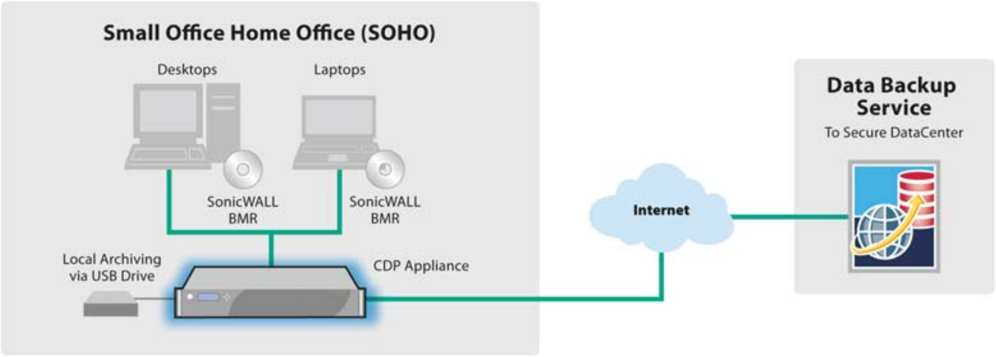
- **The SonicWALL® CDP Offsite Data Backup Service** automatically transmits and stores data at the SonicWALL Secure Data Center using AES 256-bit encryption. In the event the local CDP appliance is no longer viable, IT Administrators can easily recover the latest version of data through the CDP Offsite Web Portal.
- **SonicWALL® CDP Site-to-Site Backup** automatically transmits and stores data using secure AES 256-bit encryption to another CDP appliance at a remote site. In the event the local CDP appliance is no longer viable, IT Administrators can easily recover the latest version of data through an easy-to-use interface.
- **SonicWALL® CDP Local Archiving** capability allows IT to store the latest version of business critical data to a USB drive. Designed to help SMBs meet regulatory compliance, Local Archiving enables administrators to explore archives and restore individual files.
- **SonicWALL® CDP Bare Metal Recovery (BMR) Software** creates an exact image of an entire server or workstation including the operating system files, programs, databases, and settings. BMR's wizard-driven interface enables IT administrators to easily recover an entire system from within minutes to hours. Using the optional SonicWALL Universal Restore module, administrators can restore data to dissimilar physical or virtual hardware regardless of make, model or installed components.

- **SonicWALL® Universal Restore**, an add-on module for SonicWALL BMR software, allows administrators to quickly and easily recover server images to dissimilar physical or virtual hardware regardless of make, model or installed components—including x86 platforms. Universal Restore enables IT administrators to take the last known clean image from the source machine and import drivers associated with the new machine into the restore process. And, because the image is captured at the disk sector level, it already includes all of the configuration, application and user files, so a business network can be fully up and operational quickly and with minimal effort.

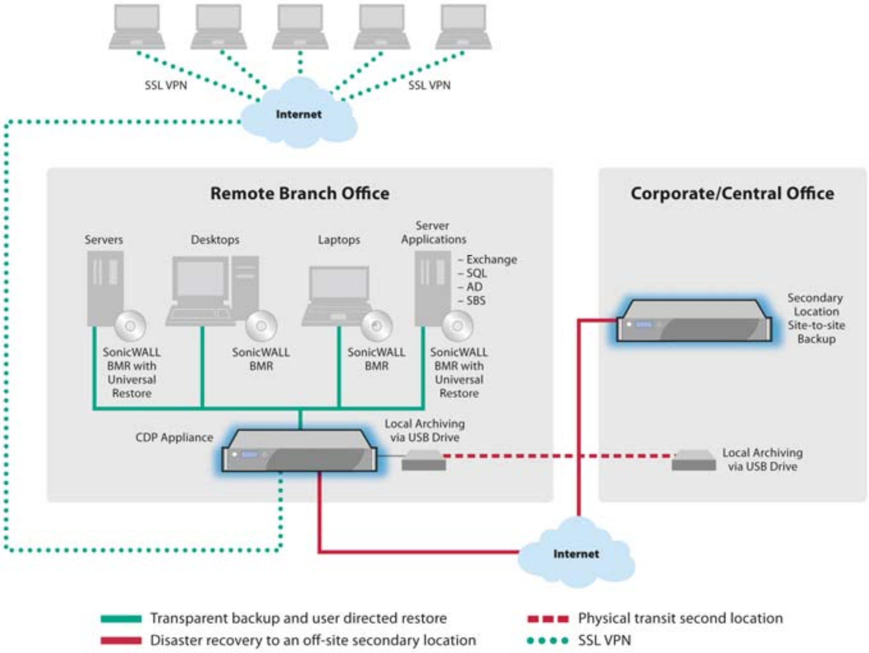
Deployment scenarios

CDP can flexibly deliver end-to-end backup and recovery for small offices and home offices, as well as distributed-environment branch offices and remote offices.

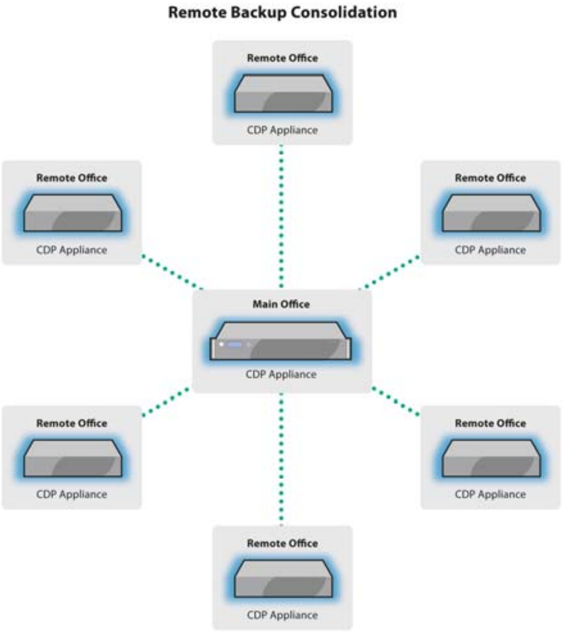
In a Small Office/Home Office (SOHO) scenario, data on desktops and laptops is transparently backed up to the CDP appliance, which is then automatically backed up to the CDP Offsite Data Backup Service using SonicWALL's state-of-the-art Secure Data Center. Additionally, the latest version of backup data can be stored to a Local Archive on a USB drive for added disaster protection, and complete system images of all workstations can be written on a secondary external media for Bare Metal Recovery.



In a Remote Office/Branch Office (ROBO) scenario, data and applications from workstations and servers at each remote office have been burned to CDs for Bare Metal Recovery. Data from workstations and servers is transparently and automatically transmitted to the local CDP appliance at headquarters. Mobile users' data is transparently and securely transmitted over SonicWALL SSL VPN to the branch office CDP appliance. The backup is then securely transmitted via CDP Site-to-Site Backup to a secondary CDP appliance at the central office. Additionally, the latest version of backup data can stored to a Local Archive on a USB drive for added disaster protection.


SSL VPN
Internet
SSL VPN
Remote Branch Office
Corporate/Central Office
Servers
Desktops
Laptops
Server Applications
– Exchange
– SQL
– AD
– SBS
SonicWALL BMR with Universal Restore
SonicWALL BMR
SonicWALL BMR
SonicWALL BMR with Universal Restore
CDP Appliance
Local Archiving via USB Drive
Secondary Location Site-to-site Backup
Local Archiving via USB Drive
Internet
🟩 Transparent backup and user directed restore
🟥 Disaster recovery to an off-site secondary location
■ ■ ■ Physical transit second location
● ● ● ● SSL VPN

To further extend and scale-up ROBO deployments in distributed remote office scenarios, a single primary CDP appliance can aggregate and centralize backups from multiple CDP appliances at multiple remote offices via SonicWALL Site-to-Site Backup.



Real-world Deployment: Potomac Hospital

Potomac Hospital in Woodbridge, Virginia, installed SonicWALL CDP appliances to provide automatic real-time data backup for servers, laptops and personal computers, and help meet regulatory compliance with privacy, documentation and audit trail requirements. Potomac installed three CDP appliances at remote building locations and another at the main building to consolidate backup information from the remote devices.

“In a hospital, there is often very little tolerance for new technology,” says Tony Davis, Manager of Network Systems, “and we cannot afford to be down for extended periods of time. In the event that we have an incident, such as a recent Exchange server problem, the SonicWALL CDP appliances allow us to get right back up and running in a few moments, protecting us from potential disasters.”

Conclusion

The survival of a small or mid-size business may depend upon its ability to recover mission-critical business systems, applications and data after a business disruption or emergency. Conventional tape-based solutions are unreliable and incomplete. SonicWALL® Continuous Data Protection (CDP) Series delivers the peace of mind that comes from knowing you are in control of your data. CDP provides SMBs with a complete end-to-end backup and recovery solution with flexible recovery options to address any disaster scenario. CDP takes the cost and complexity out of safeguarding business information by automating tedious tasks to provide a true low-touch solution. Policy-driven CDP is transparent to the end-user, ensuring that data, applications and systems are reliably protected from loss, potential disaster and malicious attack. User-directed restore increases productivity while reducing IT overhead. An ideal replacement for tape-based systems, CDP provides foolproof, intuitive continual protection of mission-critical business information without costly administrator intervention. CDP ensures that all files are available in multiple historical versions, and that all servers and their applications are protected with multiple-point-in-time versions for disaster recovery. No other solution offers such comprehensive protection while still being so easy-to-afford and easy-to-manage.