

Keeping Your Data Safe and Your Networks Connected

New Generation of Managed Appliances Provide Disaster Recovery and Improve Business Continuity

by James E. Gaskin

The fancy term is "business continuity" but the concept is simple: Keep your data safe. Make it accessible. Make it really accessible.

You've heard the first and second part of the above paragraph many times. But that last part, "really accessible," never entered the network discussion before. With a new product that links networks securely over a cellular data network, "business continuity" goes native and unwired. Better yet, these systems work more easily and are more manageable than ever.

But let me lay out the ground rules for this discussion about business continuity (the boring term) or Data Access From Anywhere, Really Anywhere (my new term).

Hierarchy of data safety and business continuity:

1. Ensure data safety by backing up all data from personal computers (including laptops) and servers, then store that data both locally and remotely.
2. Provide secure connections for remote users to access your network and your safe and secure data.
3. Take the next step and provide data connections from literally anywhere within your cellular data network.

Our order of consideration starts with data safety, because without safe and secure data nothing else matters. Then we'll discuss network access two ways: typical and atypical.

Backup Doesn't Matter - Restore Matters

Here's the painful truth: users don't think about backup unless they actively hate backup. They believe backups should be done by someone else. They will subconsciously (or consciously) sabotage backup because it doesn't matter to them one bit (or byte).

Restoring files, however, matters greatly. Users want files restored immediately. Since they want nothing to do with the backup portion of this equation, the burden falls on you.

Tape Unravels

Far too many people still think tape when they hear backup. There was a unfounded belief that tape worked adequately for decades, but falling hard disk prices changed the game. When comparing dollar per megabyte of storage space years ago, tape won against hard disks by a huge margin. The price spread was so wide that people suffered through tape's many reliability and performance problems.

While some of tape's problems improved over the years, the cost of hard disk space dropped so far companies are no longer willing to accept slow and mistake-prone tape systems for their primary backup.

Hard disk cost reductions (now pocket change per gigabyte) changed the backup equation. Disk to disk backup systems provide performance and reliability never possible with old fashioned tape. In summary, duct tape is great, but backup tape should be retired.

Backup Files As They Change

New software moves backup from a guess with tape to a guarantee with disks. Add modern Continuous Data Protection (CDP) software to your backup, and data tapes will go in the closet with your 8 track tapes.

Like many technical terms, Continuous Data Protection got hijacked by marketing and now means different things depending on the vendor. Any CDP system provides more timely backups than traditional schedule-based file backups. However, make sure you agree with your backup vendor's definition of "continuous" before buying a system.

Can the system handle common server applications, such as accounting programs (Quickbooks, Peachtree, Great Plains), sales tracking software (ACT!, Goldmine), and your favorite Microsoft applications (Exchange Server, Navision, BizTalk, Business Contact Manager, Sharepoint, etc). Network applications with databases that stay open stymie less intelligent backup systems. Make sure your backup system supports Shadow Volume Copy from Microsoft and has the ability to copy open databases without hours of extra configuration and optional (\$\$\$) software modules.

Continuous Data Protection backup systems need at least two components, and most companies demand three for adequate protection.

First, a backup file repository on the network accepts backup data from other network devices. Sometimes this job goes to a general purpose server, but smart companies use a dedicated backup appliance for better performance and security.

Second, specialized software sits on each network device and controls data transfer to the backup appliance. Personal computers (desktops and laptops) and servers run agent software. Unlike older backup software that copied changed files during the night, CDP software agents track every write operation to the client hard disk and copies the changed disk blocks to the backup appliance. The agent software works at a disk block level, not file level, greatly reducing the amount of data sent over the network to the backup appliance.

Finally, smart companies configure the backup appliance to send copies of files to a second location for redundancy. The remote location may be another company backup device or online backup service.

Store Backups Offsite

Why store backup data somewhere far away? Because in case of disaster, whether a major flood or a dropped coffee mug, your data files will be safe. Quickly restoring the files you need to run your business means the difference between recovery and bankruptcy. When your server suffers damage, the backup server beside it tends to suffer as well, so your data files better be copied somewhere else.

Remote backup file storage protects against any disaster, large or small, that may compromise the clients and backup appliance. Large disasters like hurricanes make global headlines. If your roof leaks it won't make the news but it will ruin your servers and clients. Offsite data can then be used to recreate servers and workstations once they get replaced (computers don't often recover from showers).

Tape backup users can, if they remember, store tapes offsite. But they can only restore files from those tapes when they physically insert their backup tapes into their tape drive connected to their computers. Getting tapes and new systems together physically may delay file restoration for days.

You still need locally stored backup sets. Local backup file storage makes local file recovery fast and easy. Optional Bare Metal Restore (BMR) software takes a disk image snapshot of clients and servers at scheduled intervals. When necessary, full recovery of a saved snapshot takes minutes rather than a typical workstation or server reinstall, which often takes two work days.

Wrap Up For Backup

The more management options, the better. Remote management? Makes great sense if you control remote offices large enough to have their own backup appliance. E-mail alerts in case of trouble? Of course. Central management consoles with the ability to apply policies to clients whether the clients want them or not? Absolutely, because that makes life easier for managers and ensures more clients get protected, even if against their will.

Once in place, test your backup system by restoring files regularly. Restore files to the client they came from, and to other clients, all from your storage device management interface. Verify your remote data storage location by restoring files from there as well.

Remember, users call it file backup, but they really mean file restore.

Make Your Data Accessible Virtual Private Networks Get Real

No matter how carefully you plan, some of your data is always somewhere else.

You configured a Virtual Private Network so you can reach your office network when you're not in the office. You connect remote offices together. But is your VPN flexible enough to connect employees who can't reach the office, such as during weather extremes that slow

or stop local traffic? The news won't call it a disaster, but an inch of snow in some areas makes travel dangerous. Easy employee access to your network and data means work continues even as the snow falls.

Very small companies may get by with saving shared files to an online collaboration service. But once you start running applications on your own server, that option disappears. You'll need access to data files on the servers, the ability to print back to an office printer, and a way to execute your internal Web based applications. That means you need a Virtual Private Network.

VPNs Now Less Ha\$le

A few years ago, saying "I need a VPN" out loud created great excitement among the huge network services vendors. Supporting VPNs for even a few remote connections meant expensive server equipment gear at the office plus large and difficult to install and configure client software on every remote workstation that might possibly ever need to link to the office. Add in the heavy administration overhead and fees for every remote client and you'll understand why some companies started breeding carrier pigeons for remote communications.

Technical evolution took hold, and SSL VPNs appeared. Virtual Private Networks learned to connect through a Web browser using the same Secure Sockets Layer encryption popularized by e-commerce vendors. But the early SSL versions still required expensive and complicated servers to handle connections from remote users.

The pricing trend now goes in the right direction. Hardware systems gave way to less expensive software based SSL systems which created fewer client problems than the hardware-based VPN options. Counterintuitively, progress and lower costs moved the software SSL VPN back to hardware. But now, instead of requiring large Windows servers, new hardware incarnations mean a small network appliance that hides behind the company firewall for improved security.

The VPN Appliance

Not only does the VPN appliance cost less than huge vendor network hardware or SSL VPN software applications on your existing servers, you get more flexibility. Hardware based systems needed fat client software on each remote client, and early SSL VPN vendors charged per client connection. In other words, the more you used your remote access system, the more it cost.

Now, modern SSL VPN appliances support clients without the need for special software, and they charge by the appliance, not the user. This allows companies to use remote access for regular connections like remote offices and traveling laptops, just like always. But it also allows a company to keep running if no one can get to the office, such as during bad weather. Since you can't plan ahead for weather so bad it makes travel difficult, flexibility and no per-use charges make an SSL VPN appliance a key part of your business continuity plan.

Users each get their own specific URL to connect to the SSL VPN. Yes, that makes management and user tracking that much easier through VPN management tools. For expanded access, a small client application should download transparently through the browser link after authentication, allowing remote control of desktops and access to more network resources.

Easier Authentication

Since you have no clue where your wandering laptop users may be, security takes top priority. Appliances sit just downstream from your firewall for added protection. Even better is two-factor authentication so you know the wandering laptop is still under the control of the user who carried it out the door. This level of security usually costs about \$100 or more per client, but some SSL VPN appliances include this feature. Of course, your SSL VPN appliance must support the standard third party authentication schemes (LDAP, RADIUS) and integrate with Microsoft's Active Directory and other directory services.

Remote connections assume there's some data payoff at the end of the road. Make sure your backup system at the office guarantee data files await the remote user. Teasing users with access but without data files is just cruel. Funny, perhaps, but cruel, and that doesn't fit into your business continuity plans.

Keep Your Office Open

Providing connection options allows workers to remain productive when working from home. Sometimes people want to stay home to avoid commuting or care for family members. Remote access makes a great job perk for employees in those situations. And when a real problem hits, such as winter weather that closes down travel in your area, the perk becomes a productivity lifeline and keeps your business open when other businesses shut down.

Adding up, an SSL VPN appliance will support users more flexibly for less money, be easier to configure than server-based versions, and work with your firewall for added security

Downside: no more snow days off work. Upside: your business becomes more disaster proof.

Make it Really Accessible Going Where No Network Has Gone Before

Ever needed to provide network connections to kiosks? How about connecting a first response team arriving at a location without a network? Want to link a group of users to the Internet from a rest stop by the highway?

Your T1 or DSL dies – what can you do to restore Internet connectivity immediately? What can you use for a backup?

These questions don't get asked because vendors never had a good answer for them. Why would vendors pose a problem they can't solve?

The Non-Network Network

How about the cellular data network as an answer to the questions most vendors avoid?

No, this doesn't mean use your cell phone as a laptop. It means take advantage of 3G data networks provided by every major cell phone service provider. Radio waves reach farther than broadband connections.

Imagine a small router/firewall/gateway appliance that includes a slot for a 3G PC Card. When your primary network connection fails, or when a group of users goes where broadband connections remain a rumor, you can still provide network access.

Sure, the wired data vendors promised us WiFi hot spots everywhere, but they were more than a bit optimistic. While WiFi vendors under-delivered, the cellular carriers quietly added high speed data networks to their cell towers over almost all the US.

Off-Grid Yet Managed

TV SWAT teams aren't the only groups that send out a "first response" team that needs communications. Many companies send installation teams, inventory groups, auditors, and overflow support to remote locations. These sites often lack network bandwidth, and sometimes lack network connections of any kind. Even the most mundane situations, such as opening a new remote three person sales office, can use a "connect anywhere" router when the data services provider runs their typical two weeks late for installation.

Check for two critical features: remote management, and speed. Management becomes more important than ever because the remote team will pay less attention to network niceties than a typical remote office. And everyone wants their network to be faster.

How fast? Anywhere from around 100kbps with GPRS to around 2,000kbps with EV-DO Rev A (best case). A wireless option for the cellular data router makes even more sense by providing more client flexibility (wired or wireless). And if you need to deploy a network in a park or a parking lot, flexibility is the name of the game.

It may take you some time to imagine where to use such an appliance, because your thinking has always been limited by available technology. Many companies never considered the advantages of putting networks beyond the reach of, well, networks. Now that connection technology really slips off the leash, you may find some interesting places to add a secure network router/gateway with 3G access.

Data Access From Anywhere, Really Anywhere What You're Missing Today

Many studies point out that only about a third of small and medium companies do a good job backing up their data. Notice the term was "good job" not "great job." The research firm Gartner says only 25 percent of small companies exist in a single location, meaning even the smallest companies need remote data access. Few small and medium sized businesses have a network connection Plan B to use when their network service provider fails them.

Despite user reluctance to help with any backup chores, despite the hassles of mobile and remote users, and despite the fact you may need Internet access where none exists, the show must go on. While it may seem pretentious to call Order Entry and Accounts Receivable "the show," business functions like those keep the house lights on.

Not only can you keep your data secure and available from anywhere, really anywhere today, you can do it for less money and with more management than ever before. You must manage backups, because users won't help. You must manage network connections between offices and remote employees connecting back to the office. And you must really manage a temporary network used to keep connections during an outage from your regular network provider, or when deploying a network segment far outside the reach of a broadband connection.

The old saying remains true: you can't measure what you don't manage. Now you have options to measure your increased success with file backup, data connections, and business continuity. Reliable and secure file safety and network access means your business keeps going from more places in spite of more unfortunate situations than ever before.

Better file safety and network access management almost always means more cash in hand to measure.

Adopt Managed Appliances

On one level, we've been talking about data file safety and accessing those data files from normal and unusual places for normal and unusual reasons. The fancy term, business continuity, describes the process well: keep your business running in spite of major floods or minor snow flurries.

On another level, we've been discussing the rise of managed appliances now powerful and intelligent enough to provide data file safety and network access in a wide range of situations. Big server-based applications have their place, but affordable appliances fit more situations and provide more value more flexibly.

The goal: keep your data files safe and stay connected, no matter what from no matter where. Now that small managed appliances handle big intelligent processes, you have more options at more affordable price points to keep your business up and running.

Bio

James E. Gaskin writes books, articles, and jokes about technology. In 16 books and thousands of articles, columns, and blogs, Gaskin describes ways to help small and medium businesses tame technology. Go to Gaskin.com for links to his Network World Small Business Technology column and his Technology Is Broken: How to Fix IT for Your Business video reports.