Other cool reads to check out!

- Don't Get Duped by Deduplication: Introducing Adaptive Deduplication
- Deduplication, Incremental Forever, and the Olsen Twins
- Six Fairy Tales of VMware and Hyper-V Backup

Oh, and look at the blog too!

What Most Backup Vendors Don't Want You to Know

Get past the hype and focus on simply, reliably, and cost-effectively protecting your systems and data.

Unitrends™

1

What Most Backup Vendors Don't Want You to Know

There are always a few "secrets" in any industry – and the backup and restore business has its share. Our secrets are widely known within the industry but are less well-known outside of it – for the obvious reason that none of these secrets helps the majority of the vendors in this space. These secrets are

> The cost of backup software is a fraction of what you're going to spend.
> When something goes wrong, the costs of finger-pointing are enormous.
> Online backup is an unbelievably slow recovery medium.
> Per-client and upgrade fees are the cash cow of the industry.
> If you don't protect all of your notebooks and PCs, you are risking some of your most important data.
> Tape is a great backup medium but a lousy restore medium.
> Putting your backup software on a Windows server means that you are at risk for all those computer viruses against which you're trying to protect your environment.
> Supporting heterogeneous environments is a commitment; not an afterthought.
> Replication requires either expensive dedicated hardware or a lot of resource.

The cost of backup software is a fraction of what you're going to spend

If you buy backup software with the intent of hosting it on an existing server or buying a new server, you're going to quickly discover that the cost of the backup software is simply the tip of the iceberg in terms of your capital and operational costs. You're going to need to buy an application server, an operating system, a storage controller and a lot of storage, and some pretty advanced networking. You're going to need to integrate these components in tinker-toy like fashion to create a dedicated system. Then you're going to spend a lot of time tuning and discovering that you need different components to optimize your functionality and performance. Try to save money using an older server and operating system and you're going to discover that modern backup is incredibly resource intensive – in other words, your challenge with respect to integration and tuning gets that much more difficult. And think file system fragmentation is a problem with your PC? Wait until you're regularly copying and deleting terabytes worth of data day after day, week after week, and .... well, you get the picture.

But these costs, while substantial, are nothing compared to what happens when something goes wrong.

When something goes wrong, the costs of finger-pointing are enormous.

When a problem occurs, who is responsible? Seems like a simple answer at first blush – it's the backup software vendor, right? Well – hold on there. The backup software vendor tells you that the operating system needs to be configured differently. The operating system vendor tells you that the application server is the issue. The application server vendor tells you that the storage system you purchased is the problem. And so on, and so on, and so on.

If you have a smart, hard-working, dedicated technical person working in your company who is dedicated to nothing but data protection, then at least that person can focus on pulling together the disparate vendors and fixing the problem. Conversely, you could find a company that delivers an integrated backup solution.

2

Online backup is an unbelievably slow recovery medium.

The cheapest integrated solution is online backup – sometimes called cloud-based or SaaS (Software as a Service)-based backup. And most online backup vendors do a credible job of backing up data most of the time – except for those annoying losses of service and even more annoying losses of data.

The real problem with online backup is recovery. You might not care that it takes a month or more to ship your first terabyte up through the Internet to the online backup vendor. However, most people don't have a month to wait for that terabyte to be downloaded back from their online backup vendor when a hard drive or a complete system is lost.

If you like putting money into banks but not being able to get that money back when you need it, online backup is a great answer for you.

Per-client and upgrade fees are the cash cow of the industry.

Most data protection companies charge per-client fees so that as a business grows and adds new computers there are continuing streams of revenue to that data protection company. In addition, it's common for different types of operating systems and applications to have separate charges associated with their protection as well.

Regarding upgrades, in the last ten years there have been ten versions of Backup Exec – from Backup Exec 7.3 to Backup Exec 12.5. The term for this in our industry is "monetization opportunity." In plain-speak, customers are being charged each time a new version is released. The upgrade prices for these new versions are independent of the charges for new clients and new operating systems and applications.

Of course, if your business is shrinking and you don't need new data protection features, this isn't a major issue.

If you don't protect all of your notebooks and PCs, you are risking some of your most important data.

Quite often the technical staff of a company makes the decision to protect only certain servers or even worse to protect only certain storage devices. They then create policies that all users must keep their "important" data on those servers or storage devices. They then make sure that they have state-of-the-art data protection guarding those servers or storage devices. To paraphrase Mark Twain – they're putting all their eggs in one basket and watching that basket!

If it weren't for the fact that users are human beings, this would be a perfect plan. Unfortunately, humans don't

follow rules concerning where their important data "must" be kept very well. Human beings are at times clever (the network might go down and this is an important project), lazy (I'll copy my data over tomorrow), deceitful (yes, that is the latest copy of my data on the server), and dumb (my PC won't go down.) And the technical staff typically is amused by all of this – until the company is hurt by their policies.

Tape is a great backup medium but a lousy restore medium.
Gartner Group reports 50% of tape backups fail to restore. Storage Magazine reports 77% of tape users have had tape restore failures. It's the "roach motel" solution; backups go in and they don't come out.

Tape also has tremendous operational expense and is prone to human error due to accidental over-writing, mislabeling, and other problems due to rotational tape load/unload strategies.

Tape is such a debacle as a reliable backup and restore vehicle that it reminds us of the old joke "Other than that, how was the play, Mrs. Lincoln?"

Putting your backup software on a Windows server means that you are at risk for all those computer viruses against which you're trying to protect your environment.
Most people put their purchased backup software on Windows. The reason is simple – since Windows is by far the most popular operating system, it makes sense for backup software vendors to sell their software primarily on Windows.

Due to its popularity, Windows has for years been plagued by security issues. Unfortunately, Windows is by far the leading target of computer worms and viruses. And due to its common source base, Windows servers are just as vulnerable to breaches and problems as Windows PCs and notebooks.

So ironically, one of the major reasons that you use backup software – to protect not just against disasters and hardware failure and user error but against corruption due to computer worms and viruses – is the reason that putting your backup software on Windows is a really, really bad idea.

Supporting heterogeneous environments is a commitment; not an afterthought.
It's easy to say that you support a bunch of operating systems, applications, and storage platforms – it's a lot harder to actually do it. From broad issues such as support for client-based versions of operating systems and older versions of operating systems and NAS support to the technical details of support for Windows active directory primary domain controllers or Netware BareMetal storage optimization and trustee rights to Linux domain controllers – things can get complicated very quickly.

Since many vendors tend to try to save money by focusing their R&D on the latest version of Windows, this

can quickly become a nightmare for customers that use older versions of operating systems or (gasp!) use an operating system other than Windows. It's a good idea to be very, very careful in terms of accepting claims of operating system, application, or storage platform support.

Replication requires either expensive dedicated hardware or a lot of resource.
There are two primary ways that replication can be used for data protection: array-based replication and host-based replication. An example of array-based replication is what many SANs support where you can purchase upgrades that enable one SAN to replicate to another one. An example of host-based is software that resides on your computer that allows the replication of the data on that computer to another computer.

Pretty technical, huh? Here's the bottom line. With array-based replication you're "locked in" to your storage provider for data protection and you're going to have an awfully difficult time escaping that lock – each time you want to add storage into your environment and protect it you have to pay the storage vendor. With host-based replication you're putting a tremendous load on the computers on which the host-based replication is based. And regardless, you better make sure you have a major pipe for the transmission of data – replication is pretty voracious in terms of bandwidth.

About Unitrends

Unitrends offers a family of affordable, all-in-one on-premise backup appliances that support virtual and physical system backup and disaster recovery via disk-based archiving as well as electronic vaulting to private- and public-clouds. Unitrends is customer-obsessed, not technology-obsessed, and is focused on enabling its customers to focus on their business rather than on backup.

For more information, please visit www.unitrends.com or email us at sales@unitrends.com.

Unitrends™
7 Technology Circle, Suite 100
Columbia, SC 29203

Phone: 866.359.5411
E-Mail: sales@unitrends.com
URL: www.unitrends.com