Don’t Be a Puppet of Your Backup Strategy

Are you in control of your backup strategy or is your backup strategy in control of you?

UNITRENDS

7 Technology Circle
Suite 100
Columbia, SC 29203

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

1 Don't Be a Puppet of Your Backup Strategy

Backup, despite the breathless hyperbole of many in the industry, is simply a form of insurance. What's important about your backup strategy is getting your systems and data protected in the most effective and affordable manner possible. Speaking plainly - you must be careful that you are in control of your backup strategy rather than your backup strategy (and vendor) being in control of you.

Ensuring that you focus on your company's profitability and success rather than your backup vendor's can be realized through just a few key principles:

- Backup without recovery is worthless
- Operational expense drains focus and resource from your business
- Virtualization support can't just be an afterthought
- Heterogeneity isn't just hard to spell – it's even harder to support

Each of these will be explored in detail in the sections that follow.

Backup without recovery is worthless

Sometimes it can get lost in all of the hoopla that the point of backup isn't backup at all – but recovery. If you can't recover your data, then there's really no use to go to the trouble of performing the backup in the first place, is there? Backup without recovery isn't worth a tinker's damn, a plugged nickel, a hill of beans, … well, you get the point.

There are two relatively inexpensive backup solutions for which recovery is problematic: tape and online backup. We like to call tape the "roach motel" backup solution – backups go in and they don't come out. But seriously, Gartner Group reports 50% of tape backups fail to restore while Storage Magazine reports 77% of tape users have had tape restore failures.

To be fairer about it, tape isn't really the "roach motel" solution – there certainly are cases in which tape has been shown to work. It's more of a "Russian roulette" approach to backup and recovery – you're just never sure when you're going to get surprised when you pull the trigger.

The allure of online backup can seem overwhelming – and there's no doubt that if you have at most a few gigabytes of data that most online backup vendors are a great deal. Despite the widespread reports of cloud-only-based online backup vendors losing user data, the truth is that online backup has reported recovery rates much higher than those of tape. The trouble with this type of backup is that recovery of even small amounts of data is slow.... really slow. Numbingly slow. Achingly slow.

To protect one terabyte (which could be bought for $89 during the time this paper was being written) can easily take months to upload. That's okay – after all, during that first time period you can put in place alternative backup methods (not tape, we hope!) until you get all the data into the cloud. The real problem occurs when you walk in one morning to hear your hard drive clicking and your computer won't boot. Can you really wait months to get that data back?

Operational expenses drive focus and resources from your business

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'll also need some industrial-strength anti-virus software if you're going to use Windows to host the backup software. 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 becomes 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.

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.

Finally, realize that in many cases there is a "backup tax" in the form of per-client and upgrade fees. Not only do most vendors charge you as you grow your business and you protect more servers, storage, PCs, notebooks, and workstations – but they also charge you upgrade fees as they release major new versions of their software.

Virtualization support can't just be an afterthought

We once received an e-mail a while back asking if a specific vendor's product supported virtualization. We quickly responded "No" and moved on. Of course, that wasn't the end – we got a second e-mail telling us that we were wrong. We politely inquired just how virtualization could be supported – and were told that it could occur through treating the virtual machine as just another client.

Of course, this is technically true. In fact, it works fine as long as there's relatively little load on the host (physical) system and on the virtual machines (i.e., the guest instances) executing on the host system. And there are times that this approach is clearly the superior one based on the customer's situation and goals.

Did you notice that term "…the customer's situations and goals?" It's pretty important here – because if you're focusing only on your vendor's goals you're going to end up being the puppet. How you support virtualization has to be the result of what the customer's needs are – both at the time of purchase and in the future.

Vendors that advertise 15-minute snapshots (for example) and say they support virtualization only via an agent in the host and guest operating system don't tell you that they're going to grind your system to an absolute halt due to the load placed on the system with just one or two virtual machines. Vendors that tell you to use this approach on a heavily loaded system aren't telling you that you're pouring gas on the fire in terms of compute, storage, and networking contention.

The support of virtualization means that you offer both simple solutions such as agents in virtual machines but it also means that your backup solution can scale to handle different approaches as the customer's virtual infrastructure grows. These different approaches range from native VCM (VMware Control Block) types of solutions to interoperability with third-party backup solutions designed specifically for virtualization (e.g., Vizioncore, Veeam, esXpress, and so on.)

Heterogeneity isn't just hard to spell – it's even harder to support

Virtualization is only the latest type of heterogeneity. Your backup strategy needs to accommodate for current heterogeneity as well as being flexible for the future growth of your information technology infrastructure.

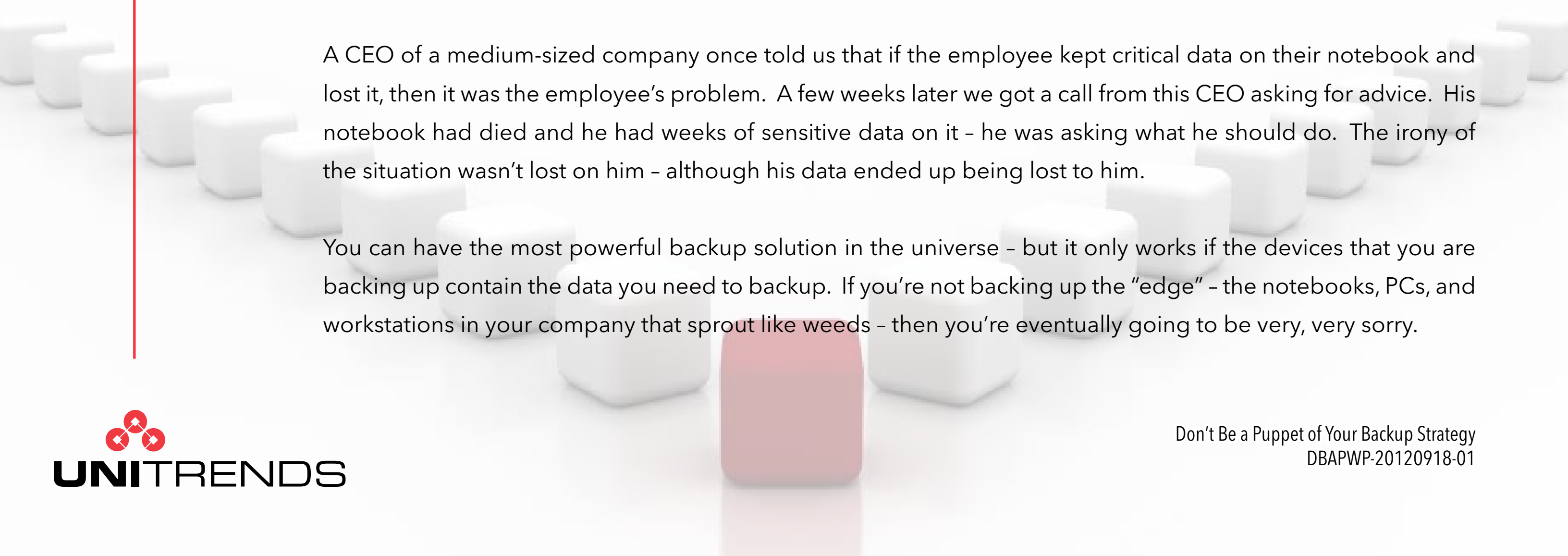
We'll talk about three classes of heterogeneity in the subsection below: different types of computers, different types of storage, and different types of operating systems.

The edge: notebooks, PCs, and workstations

There's a strong focus today on protecting your file and application servers – and it's absolutely valid. Keeping your unstructured and structured data on your servers protected is critically important. However, a lot of your critical data sits on your employee's notebooks, PCs, and workstations. And it is tremendously easier to create a policy that employees only keep critical data on your centralized servers and storage than it is to actually make that policy work.

A CEO of a medium-sized company once told us that if the employee kept critical data on their notebook and lost it, then it was the employee's problem. A few weeks later we got a call from this CEO asking for advice. His notebook had died and he had weeks of sensitive data on it – he was asking what he should do. The irony of the situation wasn't lost on him – although his data ended up being lost to him.

You can have the most powerful backup solution in the universe – but it only works if the devices that you are backing up contain the data you need to backup. If you're not backing up the "edge" – the notebooks, PCs, and workstations in your company that sprout like weeds – then you're eventually going to be very, very sorry.



Heterogeneous storage: DAS, NAS, and SAN

As noted in the previous section, it's one thing to create a policy that employees only keep critical data on your centralized servers and storage – it's another thing entirely to make that type of policy work. However, since this has previously been discussed, let's move on to other reasons that you want to ensure flexibility in supporting heterogeneous storage: DAS (Direct Attached Storage), NAS (Network Attached Storage), and SAN (Storage Attached Network.)

DAS is simply the storage that you put in your server. Everyone supports DAS. Well – wait a minute. Not everyone. SAN vendors don't support DAS. But that doesn't make sense, does it? After all, SAN vendors are storage vendors – not backup vendors –right? Well…it's complicated. [1]SAN vendors often talk about snapshots and replication with and without virtualization to make the case that they can offer data protection. And in some cases they can. Buying two SANs and placing them at different data centers does offer replication – which enables some elements of data protection, albeit at a very high price in terms of SANs and the bandwidth between the data centers. SAN snapshots allow logical copies of data to be made – they work as long as the SAN operates and you don't have worms or viruses permeating the data.

But SANs are famous for something called the "SAN island." This is when a SAN vendor sells a top-to-bottom storage and backup solution and thus has the customer "locked in." At that point, if you see an advertisement for $89 for a 7200RPM 3.5" one terabyte disk drive and decide to put it in your server, you're screwed – because your backup "solution" (the SAN) doesn't protect anything except the SAN (and that includes both DAS and NAS.) Our friend to the right visited SAN island and had trouble escaping.

Buyers with NAS devices simply need to make sure that the NAS is supported by the backup product they plan to use. There are different levels of protection – from client-based backup to direct forms of backup including both mount and NDMP approaches.

Heterogeneous operating systems and platforms

Some backup vendors support any operating system – as long as the operating system is Windows. Seriously, it's actually even worse than that. There are vendors that support only Windows servers. Even worse, these vendors don't support NASs in any form nor do they support direct-attached SANs. As long as customers are willing to not just protect only what these vendors allow but are willing to forever forego the use of any other

[1] Note: Complicated is often a synonym for "hold on to your wallet."

operating system – things can hobble along after a fashion. Or should I say – these customers can dance to the strings being pulled by the vendor.

Other operating systems say they support Windows, Mac OS X, and Linux. You need to be sure to be very specific with these types of claims. What versions? What platforms for what versions? Is the support 32-bit, 64-bit, or both? Which distribution of Linux? And on, and on, and on – the support of heterogeneous operating systems and platforms is a complex business. And particularly watch for the vendor stating they support "UNIX" – this is akin to asking someone what kind of dog they have and the answer being "mammal" – true but neither accurate nor descriptive. There are many UNIX variants out there and each has its own particular variant.

Even when a vendor tells you that they support something specifically – for example, Novell Netware – be very careful concerning what "support" really means. There's one vendor famous in our industry for claiming that they support Novell – and then their customers find they can't restore basic configurations. But this isn't limited to Netware – we see the same thing every day in Windows as well.

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.