The 5 Top Mistakes

In Architecting a BDR Solution

Could one disaster destroy your organization?

Ideally the answer is no. Ideally you have a backup and disaster recovery solution that lets you sleep well at night, knowing you can quickly spin up an accurate, high-performing clone of your environment if needed.

But reality usually isn t ideal, and neither are most organizations BDR systems.

Technology has advanced rapidly in recent years. Yet some teams are still relying on backing up physical servers to tape. Despite the siren song of virtualization, these teams are relying on costly and inefficient systems incapable of matching their organizational growth. Other teams have amassed a collection of point solutions and spend immense time trying to manage them into a cohesive and efficient ecosystem.

As their amounts of storage keep increasing, sometimes 15 or 30 percent a year, these teams struggle to make their old BDR system work. Others find themselves dealing with unacceptable levels of downtime, despite multiple solutions. Add in the fact that your typical team might be dealing with a mix of some physical servers, virtual machines from different hypervisors, varying types of storage, and a few workloads in the cloud, and their confusion increases.

Teams are realizing that their data protection strategies must change. Uptime is still the goal, but SaaS applications, cloud systems and other assets need to be protected. Security is vital in the age of cyberattacks, which makes speedy recovery more important than ever in successfully defeating attacks like Ransomware.

All of this adds up to new challenges that can t be solved with old strategies. Yet this kind of advanced, secure BDR is far from reality for many teams. Sometimes this is because they re mired in outdated solutions; other times a few mistakes have become baked into their organizational practices.

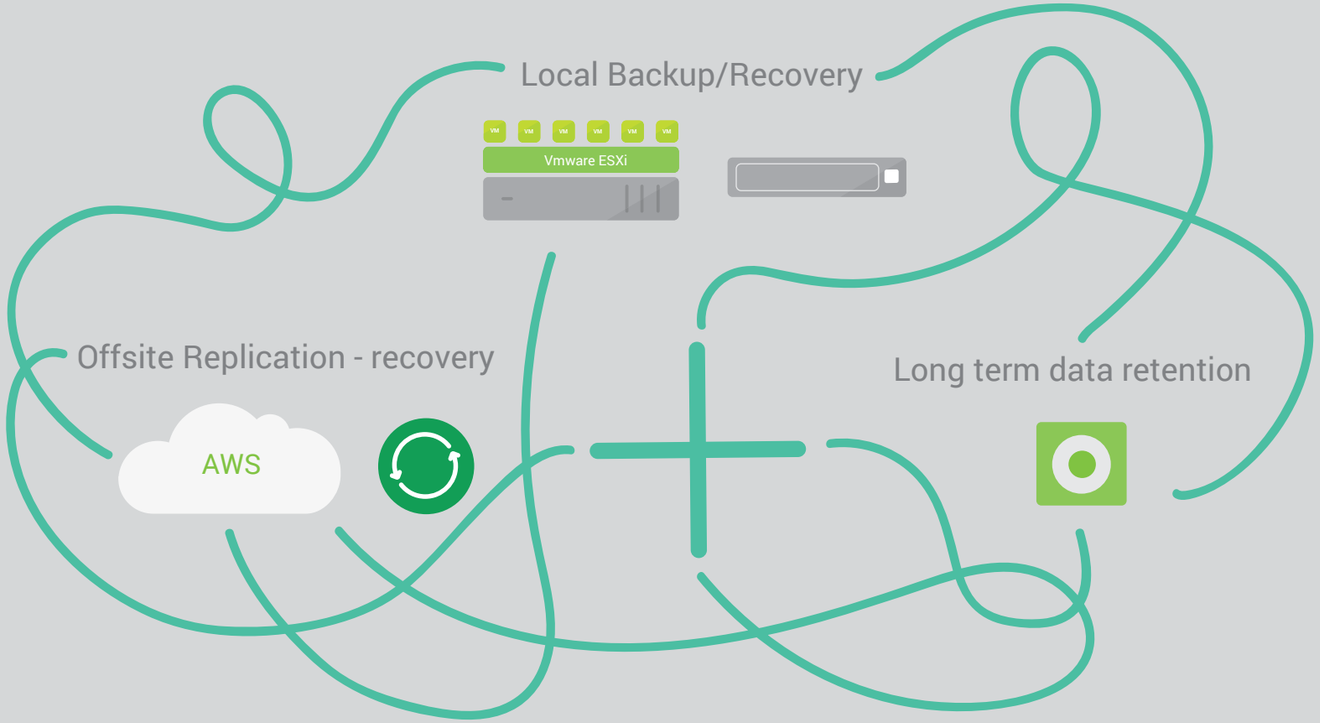
The 5 mistakes listed here are destructive to IT health, yet common across teams. By embracing new tactics and new technologies, organizations can strengthen their ability to recover from disaster and revitalize their productivity by leaving chaos and inefficiencies behind.

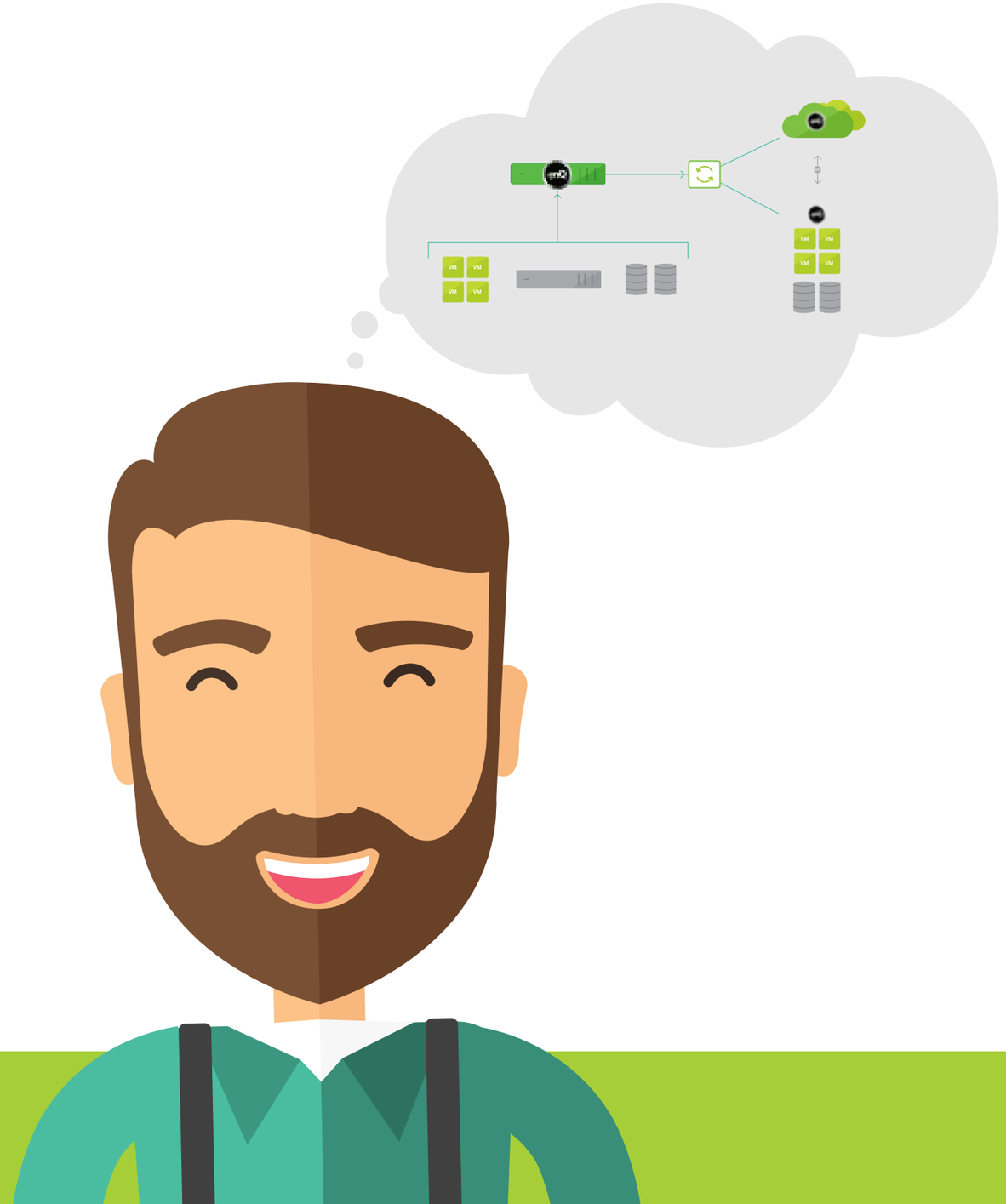
Mistake #1

OVERLY COMPLICATED SOLUTIONS

Here s a scenario you might be familiar with. Let s say you work for a company with a major footprint: multiple sites, multiple datacenters, and quite a few cloud resources to boot. As a result, backing up your data is one of the most arduous parts of your job. It s complicated and tedious, and takes you away from your other responsibilities for far too long.

One reason it s so bothersome: you have different point solutions for your VMs, your physical servers, your archiving solution and your workloads in AWS. That means dealing with different vendors for each, as well as different licensing, different pricing, different hardware and software updates. And despite your dedication, the solutions don t always work well together, leaving some of your assets at risk.





Solution #1

SIMPLIFY AND UNIFY

The idea of having just one vendor for all your backup and recovery needs might have been a pipedream once, back when conventional solutions were technically incapable of backing up your abundant portfolio of data. But times have changed and that dream is easily within reach now. Advanced solutions can provide one-stop-shopping for all your BDR needs, including long-term archiving, local failure recovery and protecting cloud data. You ll save time and have a solution that functions as one cohesive system and cut all that tedious management into something much smoother and easier.

One caveat: some vendors say they can take care of everything, and then exhibit some weaknesses down the road. Before you invest in a new solution, make the vendor prove they can fit your needs. Ask for proof of concept in the form of an actual demonstration. Also ask for a full trial for 30 days, and make sure that thorough training is included. Be sure that your one and only really is the one and if you feel misled, ask for a return.

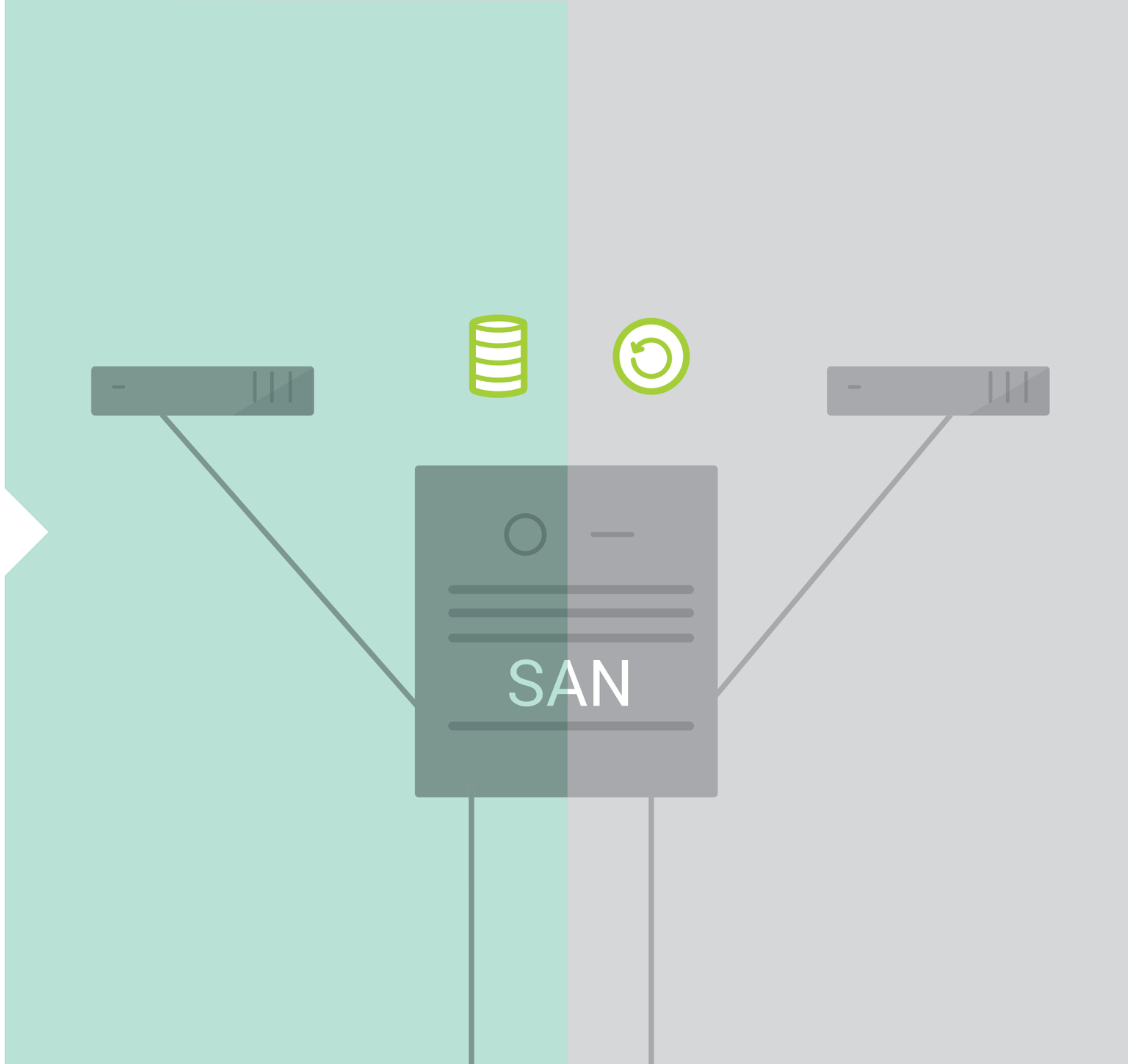
Mistake #2

USING PRODUCTION SYSTEMS/STORAGE AS A BACKUP TARGET

Let s say you re working at a different company now. As you begin to investigate the system, you realize the team has opted to leverage free space on SAN for backups. You understand why they did this; they went with a software-only solution that leveraged the production environment to save money.

That weekend a SAN outage wipes out all of your backups. You now have no replicas, and are forced to send off the hardware to have data recovered. This is exorbitantly expensive in terms of money and time.

This is a valuable lesson that often comes with a painful price: take a good look at any shortcut that promises to save money. Yes, it s tempting to trim BDR costs here and there. But often the theoretical savings are dwarfed by the cost of an ensuing disaster. In the above case, backups that had been deployed safely in an isolated environment would have been available for a quick and standard recovery.



Solution #2

SAVE MONEY THE SMART WAY

Every team is working within a budget. But most BDR shortcuts like stashing backups in your production environment are really a short road to wasted resources. The next time you eye a software-only solution or strategy promising to save money, do an apples-to-apples comparison with an all-in-one solution. Chances are, by the time you calculate additional expenses, the price is probably the same. You re not saving money so much as spending it at a different point in time often with more risk.

To really lower your costs, calculate your RPO (how much data can you lose?) and your RTO (recovery time objective.) Once you create those expectations, look for a solution that can achieve those two standards. If you re choosing between a mediocre but budget-friendly solution and a premium solution, buy the latter in phases. For instance, you might spring for local protection first and spend on offsite protection later. This will always serve you better than buying an inexpensive solution, while still keeping you in budget.

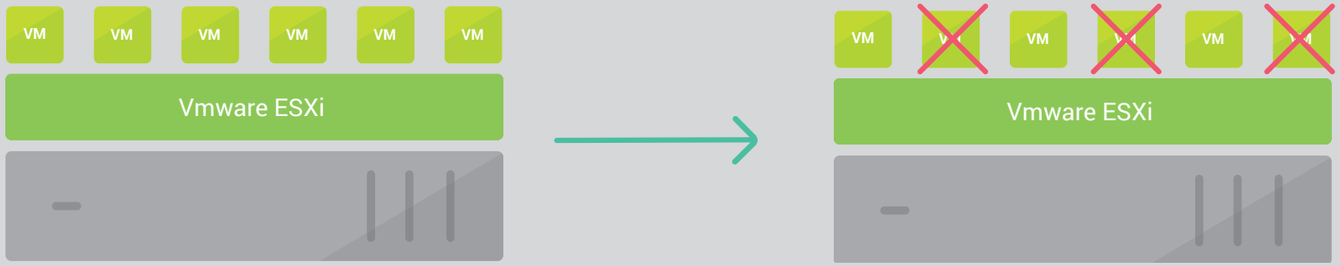
Mistake #3

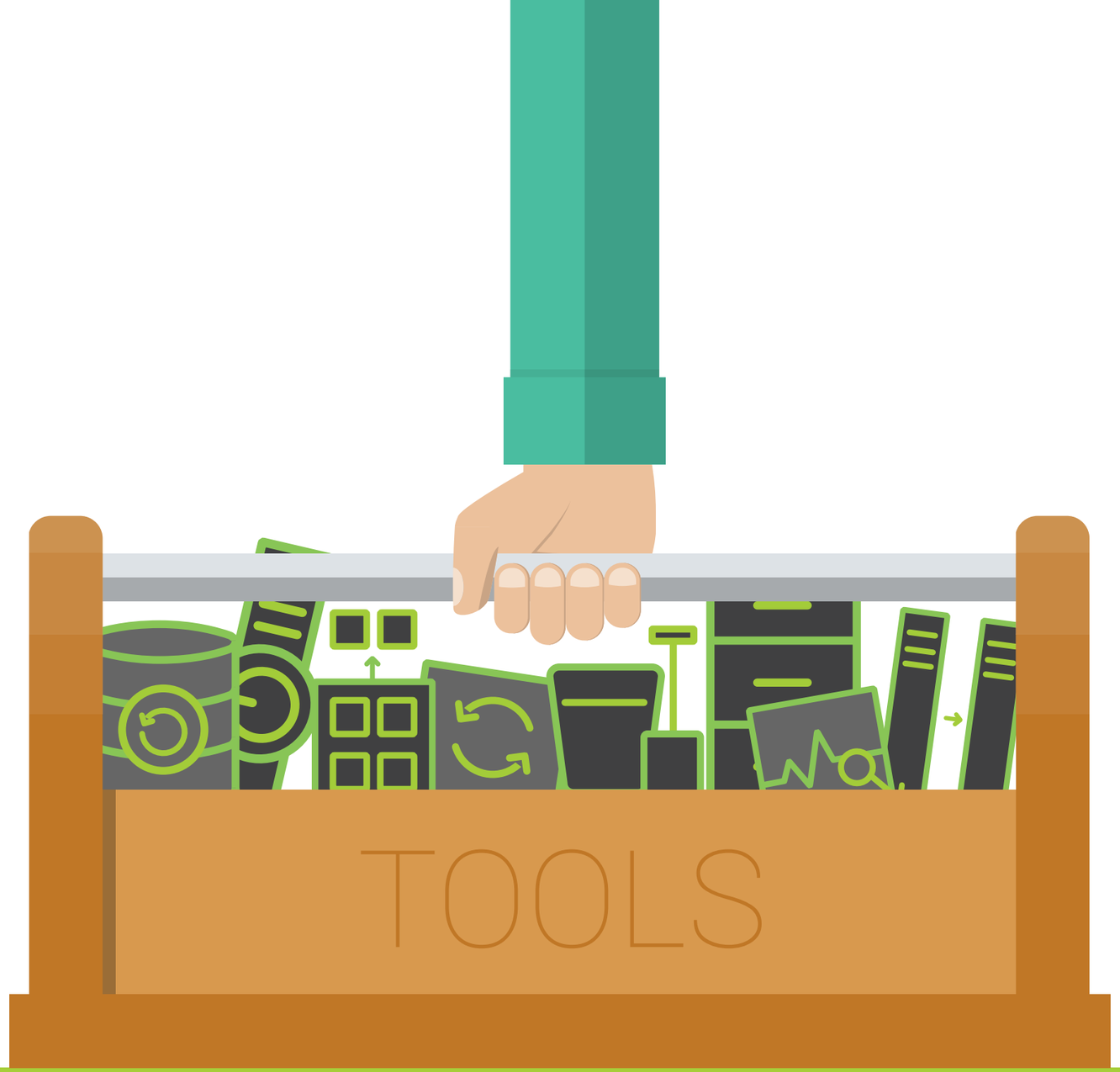
PARTIAL VS. FULL SITE RECOVERY

If you ve done your time in the BDR trenches, you ve probably encountered a team that s decided partial recovery is all they really need. It sounds smart on the surface; some data and systems are more important than others. But this doesn t always work out as planned.

We knew a team once that deployed an OS change that caused a cascading event. Two servers went down in 10 minutes. Their solution could handle that; it wasn t a problem. Yet the issue crawled from OS to OS to OS and within an hour, 20 servers were down. Their BDR solution wasn t designed to recover everything; by the time they booted up the third server, their recovery solution was at capacity. It had been designed to back up everything, but not to recover everything at least not all at the same time.

The team was now in the unenviable position of having to decide what had to be online and what could stay offline as they recovered. This was not an easy discussion. Together they had to debate every piece of the pie: should they prioritize the domain controller and exchange server and not a critical file server? It was a painful process, one which taught them that partial recovery is never enough.





Solution #3

GO FOR FULL RECOVERY

Get the right solution that can recover everything. This is the age of 24/7 uptime. You need to invest in a solution that can make a remote copy of all of your apps and data, and has enough horsepower to keep everything running local and remote while delivering production level performance.

This evaluation should be an important part of your trial. Guided by your RTO, demand that the vendor demonstrate the ability to spin up the entire environment at one time. Many will focus on just a few applications, or offer a canned demonstration. Request to see a full demonstration that looks like your environment. Only then will you be assured of true protection.

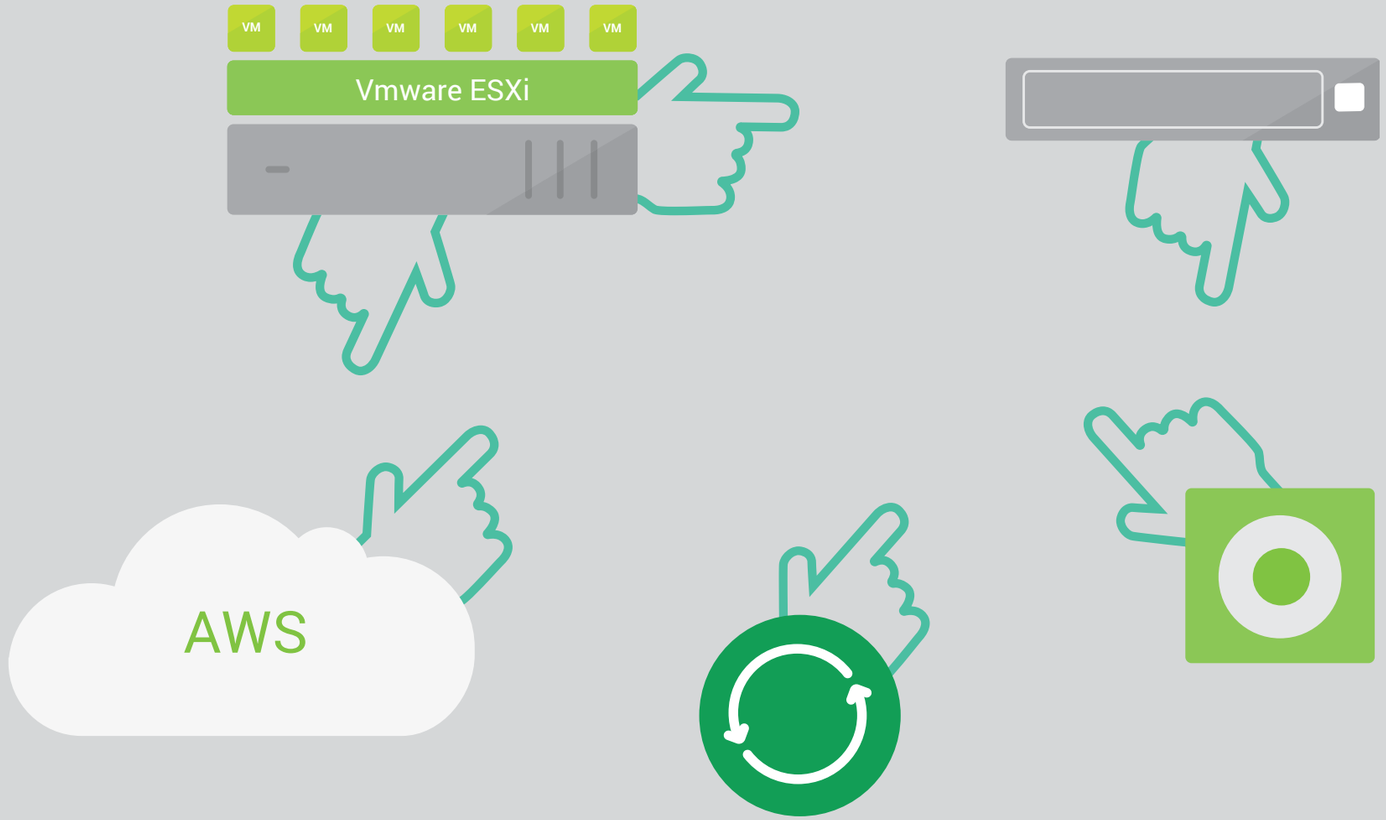
Mistake #4

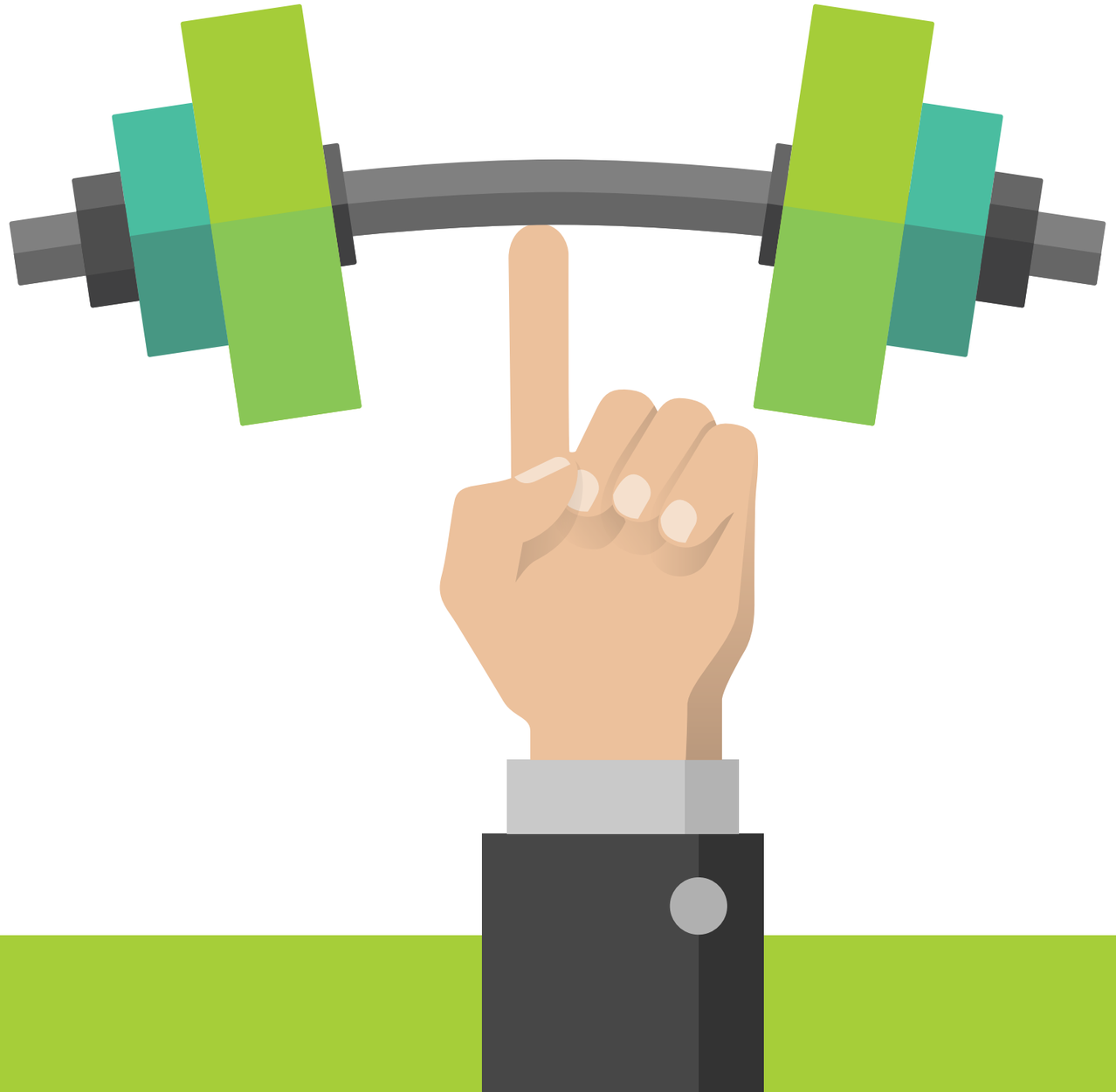
MIXING PRODUCTS AND VENDORS

If you re using a mix of vendors for backup and recovery and Quorum s State of Disaster Recovery Report 2016 says 64 percent of you are you ve probably had the following happen.

Your system goes down. Naturally, you call up one of your vendors and your contact says, That s not us. It must be your network guy. You call your network guy and he says you guessed it, That s not us. And so it goes on down the line, one finger pointing at the next vendor until you're standing in the middle of a circle of blame and your system is still down.

That s what happens when you mix and match vendors. They all blame someone else whenever there s a malfunction and it s very easy for them to do this, because without a conversation analyzing how the solutions are working together, each can claim ignorance on the details of your tech stack. Even worse, these disputes can drag on for months while your team tries fruitlessly to uncover the root of the problem and get it resolved.





Solution #4

EMBRACE THE POWER OF 1

Working with just one vendor does simplify your process, as we noted earlier. But it also resolves your problems that much faster when something s not replicating or backing up correctly. If there s only one company only to turn to, they have the ability to understand how each component of your backup and disaster recovery architecture is working together.

Another caveat: if your one vendor houses a number of entities under their umbrella, you may not always get the unified, inclusive support and resolution you need. You may be fine with that approach. But if you prefer OEM hardware, support and software directly from the company, ask these questions:

Where is the support team located? Are they on a different continent? Is the vendor a reseller who only does Tier 1 support? Does the vendor offer call back support where you might wait a few days for a response, or can you call and speak to a knowledgeable person?

Where is the development work being done? Does the vendor use third party developers? If so, are there internal developers you can leverage? It ll be much more helpful if you can bring your problem to them directly and ask them how the software might be causing that issue.

Who makes the hardware? Is it whitebox hardware? Is there a hardware warranty?

Ultimately, this is about your comfort zone, so find out in advance just how unified the solution is.

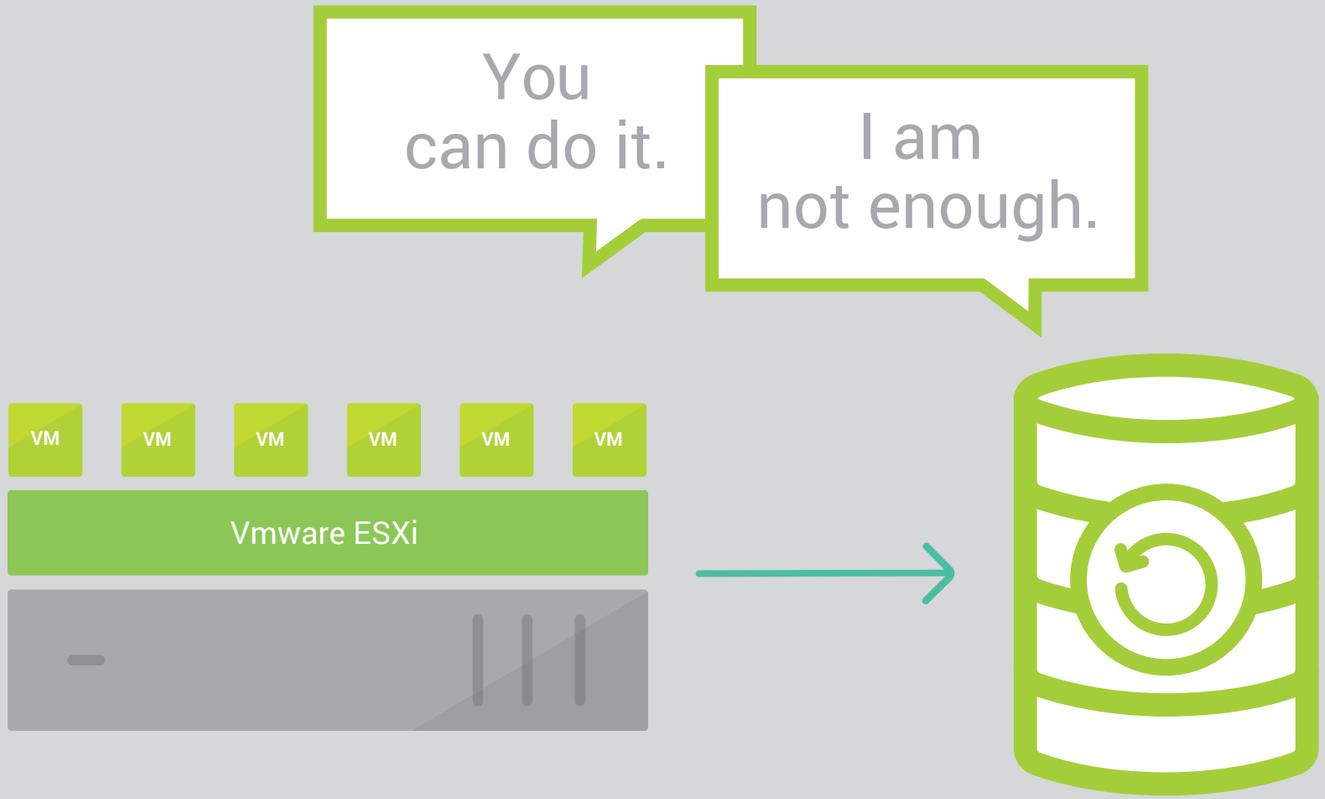
1
2
3
4
5

Mistake #5

SCALABILITY LIMITATIONS

Let s say you want to add more VMs to your environment. Or maybe you d like to add a little storage to your SAN, or scale out your production environment. We call this data/VM sprawl and it s a natural occurrence in most organizations.

Assuming that your production environment is going to grow eventually, is your backup solution positioned to grow with it? The importance of scalability gets a lot of lip service, yet a surprising number of companies don t consider it early enough. But a growing production environment needs expanding storage, and that means a growing backup solution as well.



Solution #5

DEMAND ROOM FOR GROWTH

Realizing you ve invested in a BDR solution that can t grow with you is always a sinking feeling. Look for a solution that can not only expand as needed, but grow independently of your VM and ask these questions.

Is it built to scale? What calculations have gone into the yearly growth is the sales rep assuming five, ten, thirty percent growth for you?

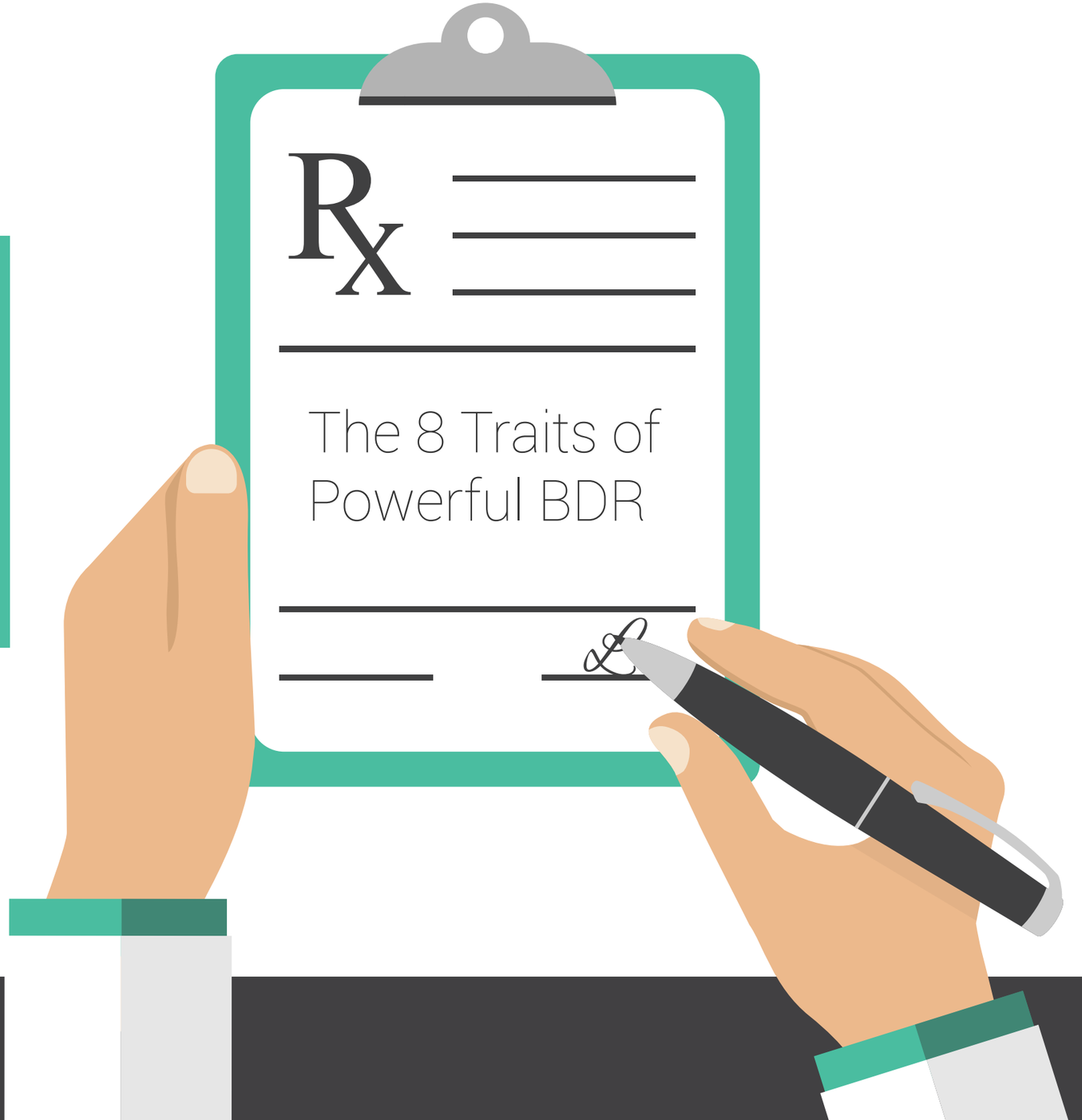
What does the licensing cover in your BDR model? Is it based on a core license, sockets, the flat number of servers you re protecting? Don t let this stay ambiguous, or you could be gouged when you hit a certain number of VMs. Ask up front to have extra room for growth built in, such as a free core license or extra sockets.

What if you go from 10 terabytes this year to 15 terabytes next year? If the sales rep doesn't have a quick and clear answer for you, there are two possibilities: the vendor hasn t thought about it or worse, the vendor wants to get you into a small solution - in the hopes you ll come crawling back and ask for a bigger one.

Prescription for Protection

If there s one good thing about the incessant cycles of change in IT, it s the ongoing opportunity for improvement. While your IT leaders may have made mistakes in the past with their backup and disaster recovery choices, there is always room to pursue a more advanced solution and a smarter architectural strategy.

As you embark on migrating to a new solution, or improving your existing BDR world, keep the following 8 Traits of Powerful BDR in mind.



THE 8 TRAITS OF POWERFUL BDR

01 **Simple.** Complex is the opposite of sophisticated in BDR. Too many solutions will eat up your time and budget while weakening your overall resilience to disaster. Keep it simple, so you can act swiftly and decisively when calamity strikes.

02 **Reliable.** Your BDR solution must sit apart from production, to keep any problems in one area from impacting another. Your backups are your final line of defense; give them the protected environment and automated testing they deserve, so you know you can turn to them no matter what.

03 **Comprehensive.** If your BDR strategies center on protecting data, it s time to expand the goalposts. Think in terms of protecting your server and applications as well, and factor that into your solution evaluation. You need a solution that protects everything.

04 **Unified.** Surrounding yourself with multiple vendors is an invitation to chaos and wasted budget. Find the one vendor who can handle it all: VMs, physical servers, cloud resources, archiving, automated testing, outage monitoring and anything else on your wish list.

05 **Robust.** Unless stagnation is part of your 5-year forecast, you need a BDR solution that can grow with your company. Don t get locked into any new plan until you know the solution can will assist your success, rather than hindering it.

06 **Cloud flexibility.** Physical servers aren t going away, but the cloud offers specific benefits that are transforming organizations of every size. Look for a solution that can adapt to your needs and deliver DRaaS, hybrid cloud and any other arrangement that could work best for you.

07 **Fast.** Settling for hours of downtime is settling for serious loss in terms of reputation, sales and more. If there's one quality that signifies strong BDR, it s the ability to get you up and running within minutes. Nothing less is acceptable.

08 **Secure.** As criminals grow more skilled, advanced security must extend deep into your BDR system. Be sure your backups are encrypted and protected, whether local or offsite, and that your controls are architected with the latest threats in mind.

EMBRACING BDR EXCELLENCE, EMBRACING GROWTH

Risk is part of every organization s future. To succeed means teams must innovate, explore and occasionally fail. It also means teams must recognize when yesterday s solution is no longer serving them, and move on to a future of advanced technical capabilities. As the business world asks every organization to perform at a fast, safe and consistent level, backup and disaster recovery systems have become an enabler of performance and profit. Take an unflinching look at your system and identify the opportunities for stronger reliability and security. By architecting a stronger web of protection, you'll empower your business to compete with confidence.

Quorum®
1-Click Instant Recovery