The Ultimate DRaaS Best Practices Guide

4 Secrets to Making DRaaS Work For You

Quorum®
1-Click Instant Recovery

If there’s one word we don’t associate with backup and disaster recovery, it’s leisure.

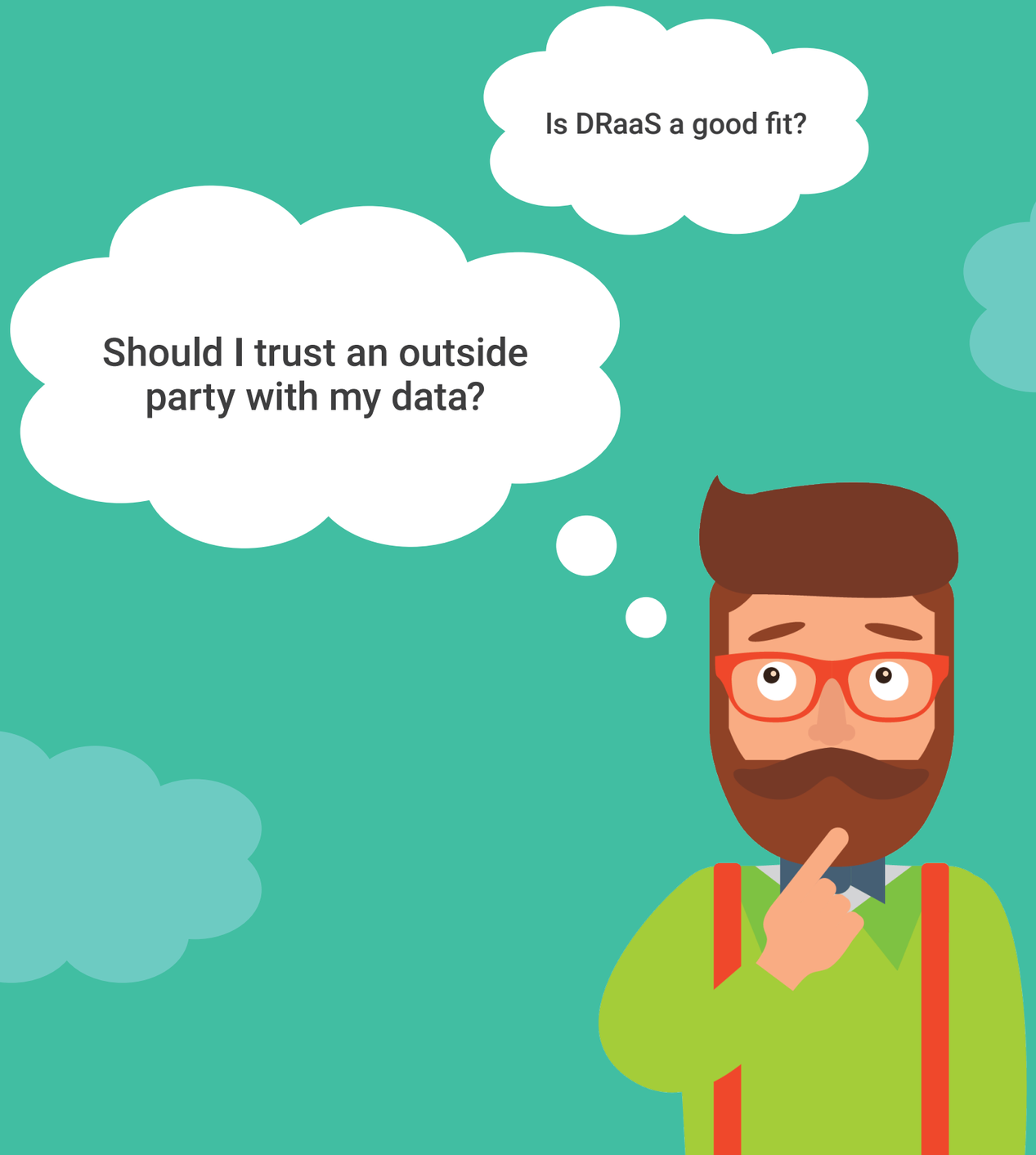
As in, the leisure to get back to the parts of your job you enjoy; the leisure to get strategic and innovative and find new ways to create business value; the leisure to leave work on time and rest easy in the knowledge that even if disaster strikes, your systems, apps and data are protected.

If you’re used to laborious backup processes and uncertain recovery, BDR that qualifies as simple and safe might seem like a fantasy. But Disaster Recovery as a Service (DRaaS) can remove significant maintenance, headaches and stress while providing the assured protection that comes with advanced technology and BDR expertise.

In these days where it seems everything IT must become an “aaS” of some kind, it was inevitable that disaster recovery would jump to the cloud. But DRaaS is no fad. A powerful option for organizations of all sizes, managed/hosted BDR services means organizations can protect their assets in a flexible, cost-effective way—as opposed to assuming the burden of building additional data centers and equipping them with servers, storage and staff.

Yet while more and more teams are adopting DRaaS, others are stopped by two issues:

- They don’t know what DRaaS can deliver and how to evaluate providers. After a lifetime of handling their own backups and owning their own datacenters, the idea of entrusting their data to an outside party is unnerving.
- They aren’t sure if DRaaS is a good fit for them. They want their new venture to deliver all the benefits they’ve heard, from cost savings to agility to fast recovery. But with many teams operating under a fixed budget, they can’t afford to spend their budget on a solution that doesn’t work with their needs.



THE BENEFITS OF DRaaS

Most IT teams face similar challenges when it comes to dealing with disasters. The business expectations for continuity don't quite match your capabilities. Employee morale can take a nosedive when staff are faced with recurring downtime; your partners can become resentful when your outage paralyzes their performance.

The world of apps and security requirements keeps growing more complex, yet your budget may be staying flat. Your team might be staffed by people who haven't yet lived through a major disaster, which means you're short on hands-on expertise. And sometimes your C-suite leadership just doesn't prioritize the need for fresher and more efficient BDR solutions.

DRaaS can solve or mitigate many of these challenges. In addition to eliminating physical data center costs, virtualization can reduce storage requirements through deduplication and compression. It can even the playing field for small and medium-sized businesses who don't want to invest in a secondary and tertiary backup location. Even enterprise organizations are vulnerable to theft, floods, fire and other disasters when their backup data center is close to the primary data center. By relying on an experienced provider, teams can enjoy the best technology and skills in the backup and disaster recovery field – while staying focused on other initiatives.

Is DRaaS Right for You?

If your current DR arrangements are adequate for your needs – they support mission-critical systems, keep your buyers buying and your workforce working, and they provide abundant data storage – you may not think DRaaS can benefit you. And if your team is mired in expensive investments, long-term contracts or legacy applications tied to certain infrastructures, you may not be ready to adopt DRaaS just yet. But a DRaaS arrangement may make sense if:

Your recovery times are slow. Moving into the world of virtualized BDR can transform hours and days of waiting for recovery to mere minutes – something that's not just impressive, but necessary in today's world.

You know you're not ready for that next big disaster. It's going to happen eventually, whether it's a breach or a hurricane or human error. If you know your backups aren't secure, that your staff is inexperienced in disaster management, that your system is too complicated and uncertain for immediate, assured recovery – you need to put your future in the hands of experts.

Your team lacks time or skill. Instead of asking staff to spend their days managing backups or creating complex configurations, you can put them back to work on their core mission while your DRaaS provider compensates for the skills currently missing on your team.

You want to upgrade your backup and disaster recovery but your IT budget isn't growing. DRaaS can let you pay as you go, without a colossal investment up front. Flexible short-term contracts can make an arrangement even friendlier to your budget. Instead of overpaying for unused resources, or worrying about buying enough servers to keep up with your growing data, you can agree on a fixed monthly fee.

DRaaS can make your IT life simpler and safer– but to maximize the benefits, you'll need to understand the best practices for planning your strategy, implementing the solution and managing your provider relationship.

According to Disaster Recovery as a Service Market, The DRaaS market is expected to grow from USD 1.68 billion in 2016 to 11.11 billion by 2021.

4 Best Practices for Successful DRaaS

1

Understand Your Objectives

Things change quickly in IT.

If you've been using your current BDR system for a while, or haven't done a recent risk assessment, it may be time to reevaluate your systems, applications and data.

Which are really mission critical and which need the most protection? What systems might be able to afford a delay in recovery? These categories will shift over time, so don't rely on what used to be true. Take a look at where the demand and value is now.

Next, identify the risks you're facing – from storms to hardware failure to cybercrime. Where are the downfalls in your current system? What's your biggest recurring problem? Biggest vulnerability?

Now consider your business needs. Is your company planning on expanding? Are you in a position to invest in new data centers or does it make more sense to play it by ear? Look at your stakeholders too. What kind of internal SLAs do you have with your business owners or customers? What apps do they rely on? Do they have conflicting needs? For instance, your IT team may be more focused on operations and integration while your executives will prioritize the continuity and security that preserve brand image and keep revenue flowing in.

All of this will help you devise accurate recovery time objectives (RTO) and recovery point objectives (RPO) and categorize your assets into tiers of DR classifications. At this point you'll have a clear idea of what you need from a DRaaS provider.

2

Evaluate DRaaS Providers

With so many offerings in the DRaaS landscape, you'll need to avoid the vendors that overpromise and underdeliver.

Too often a DRaaS provider will deliver a solution that doesn't work with your current investments – creating another layer of complexity instead of simplifying your current system.

To make sure you find a provider that can make good on their promises and meet your expectations, you'll need to ask the right questions.

Once you've found a provider who seems like they can deliver DRaaS that's fast, simple and secure, ask for proof. A reputable provider will be able to offer documentation like audit reports, references and attestations, team bios and even copies of warranties to show you the staff and technology that will be managing your backups and recovery.

IMPORTANT QUESTIONS TO ASK

- What kind of speed in recovery can they deliver? Can they guarantee availability for all your stakeholder needs – from business units to customers to employees and partners?
- How fast are the backups? Can the backup environments perform as fast and well as the primary environment?
- How easy will it be to failover? Will it take just the click of a button or will you need to follow a complicated process involving multiple steps – steps you may not remember months after training?
- How easy is the solution to use? Do they have an integrated dashboard where you can get an all-in-one overview of your entire backup and disaster recovery ecosystem? How easy is it to failback or enroll applications?
- Do they offer automated backup testing? What about testing the entire system? Will they work with you to develop and test your DRaaS plan so you know it will work when you need it to?
- Can the vendor reconstruct an image of your data from your chosen point in time? How far back are backups available in calendar terms? Can they support file-level recovery?
- What kind of security can they offer? Are their backups encrypted? Will your infrastructure share servers and other devices with other organizations?
- Can they make it easy for you to meet compliance regulations? Whether you're subject to HIPAA, PCI-DSS or other standards, your auditors and regulators will require documented evidence of your security controls, risk assessments, third party validation and testing. Can your provider support that?
- What kind of support do they offer? Will your call go to a third party center in another country or the actual engineers who built the solution? Will you be able to speak to a real person when you call in the middle of a crisis – or is the support callback only?

Negotiate A Service Level Agreement That Works For Your RTO

An SLA changes the provider's promise into a binding agreement.

While recovery times are at the heart of your SLA, it can also map out your arrangement for monitoring, administration, replication systems, failover support, training, prioritization and recovery tiers, process workflows, security and other components of your partnership.

Now is the time to review the risks, stakeholder needs and RTOs that you outlined earlier. Be clear on how your provider defines continuity and recovery, such as ensuring an application or system is be available to end users. Look at your recovery tiers and make sure the SLA is explicit in what the provider will guarantee.

Example:

Hot/Tier One: These would be your critical assets and workloads, requiring near-instant recovery and constant availability. Number of tolerable outages: zero.

Warm/Tier Two: High availability is still important for this group, with 1-2 outages per year of no more than a few hours.

Cool/Tier Three: For this group, you might accept 24-hour recovery and 2-3 outages per year.

Before you finalize the SLA, make sure your DRaaS solution is still cost effective. If the provider is going to add on costs for every feature and nickel and dime your team, instead of an inclusive quote that meets all your needs, you may be in for some unhappy surprises down the line. A good provider will keep pricing and licensing straightforward and clear, and that should extend to the SLA.

Also important to include: the terms of your compensation or credit if the provider fails to meet their business obligations.

4

Start Smart– And Keep Testing

Rather than jumping right into your DRaaS arrangement, consider a phased migration.

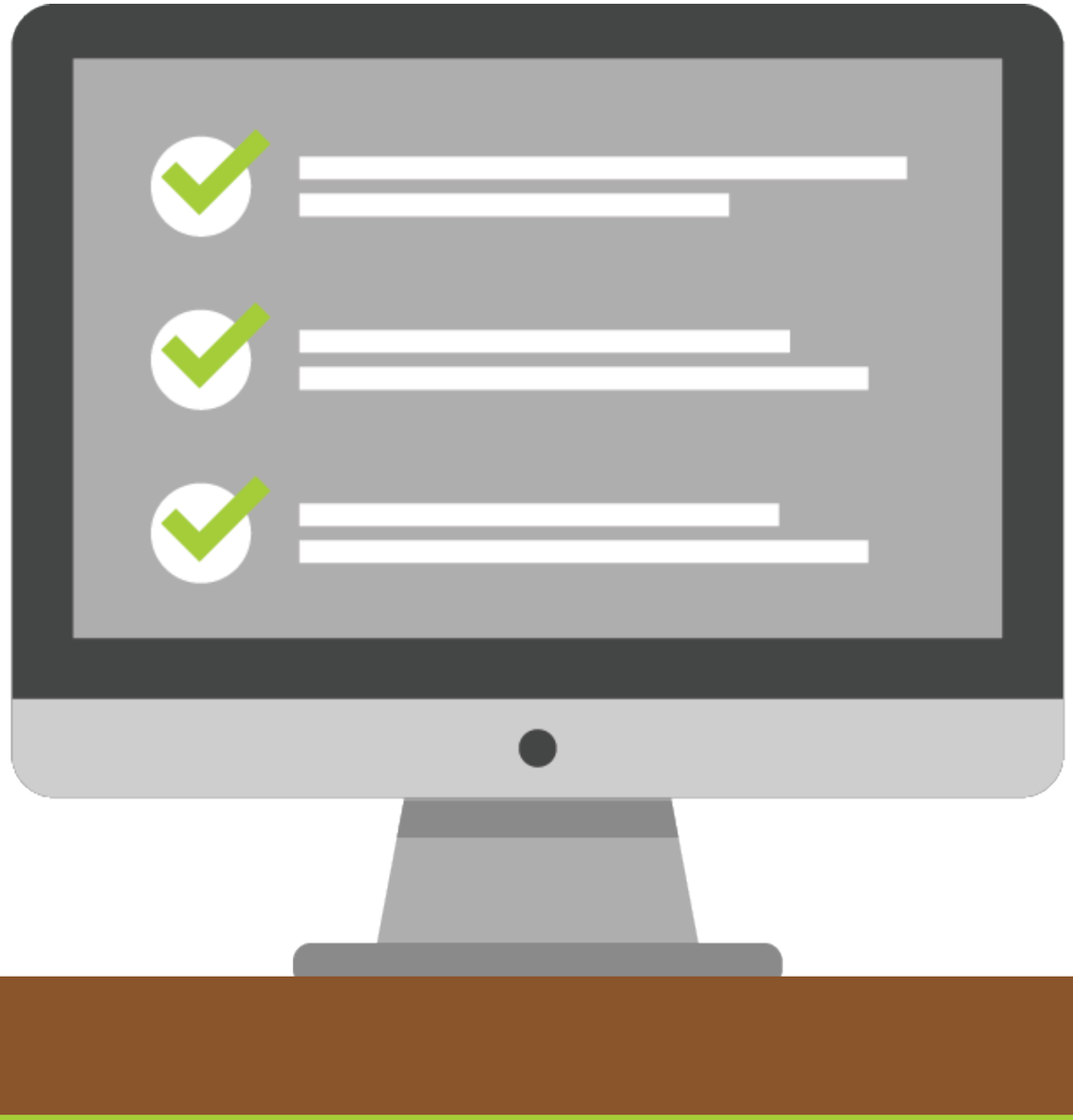
By offering up select data and applications for the first six months, you can evaluate your provider in action without an upheaval to your infrastructure.

That evaluation will take certain forms. You may or may not have a genuine disaster to grapple with during the initial months. One way to safely and accurately assess the strength of your new solution: testing.

While testing has always been a weak link in the BDR chain, many teams overlook it even more after handing off their disaster recovery to a cloud provider. But because these are still your systems and assets in play, you'll need to develop an efficient plan to test the reliability of your business continuity and disaster recovery.

Work with your provider to launch a realistic test. For instance, you might pull the plug on a server and see if it can fail over properly. Simulate a natural disaster or breach and see how long it takes to get the application running in the cloud. Pretend that you've been attacked by ransomware and check that you can restore fast enough to thwart even a tight ransom demand.

Some good news here: while you may have found testing burdensome in your physical BDR days, virtualization can make testing significantly easier. You can even create a virtual isolated test network and create application copies without impacting production. Again, this is one reason DRaaS gives many teams a greater sense of confidence: their ability to recover shifts from theoretical to proven.



PROTECTION WITHOUT COMPLEXITY

The technology industry has come a long way since the days when disaster recovery was a privilege reserved for the biggest of IT budgets. DRaaS has extended sophisticated tech and experienced DR staff to organizations at a fraction of the price. For many teams, this is the ideal way to avoid the cost and brand damage of a badly managed disaster while benefitting from stronger security, easier management and faster recovery. Is DRaaS for you? Give it a try – and you may find the perfect solution for your backup and disaster recovery needs.

Quorum®
1-Click Instant Recovery