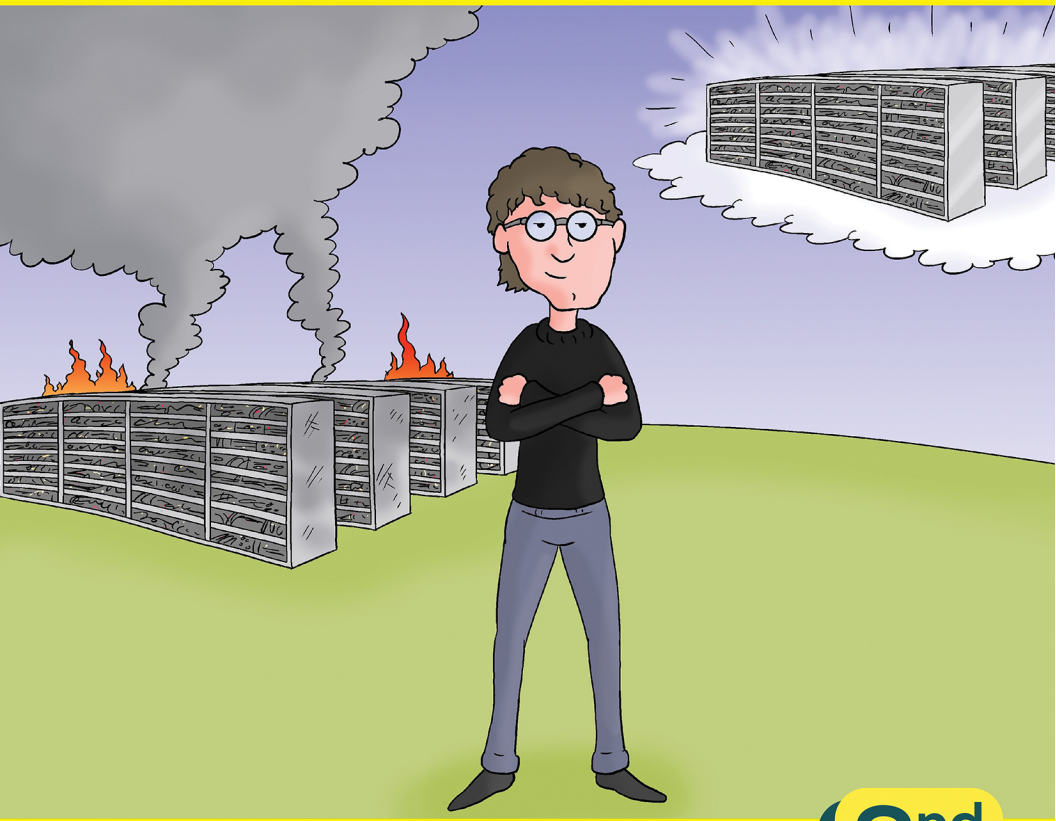
ConversationalGeek®

Conversational Disaster Recovery as a Service

By Brien Posey (Microsoft MVP, Commercial Scientist Astronaut Candidate)



In this book, you will learn:

- The basics of Disaster Recovery (DR) and Disaster Recovery as a Service (DRaaS)
- Why companies need to be moving from DR to DRaaS
- What to look for in a Disaster Recovery as a Service solution

2nd Edition

Sponsored by

VEEAM

Sponsored by Veeam

Veeam® is the leader in backup, recovery and data management solutions that deliver Modern Data Protection. The company provides a single platform for Cloud, Virtual, Physical, SaaS and Kubernetes environments.

Veeam customers are confident their apps and data are protected from ransomware, disaster and harmful actors and always available with the most simple, flexible, reliable and powerful platform in the industry. Veeam protects over 450,000 customers worldwide, including 81% of the Fortune 500 and 70% of the Global 2,000. Veeam's global ecosystem includes 35,000+ technology partners, resellers and service providers, and alliance partners and has offices in more than 30 countries.

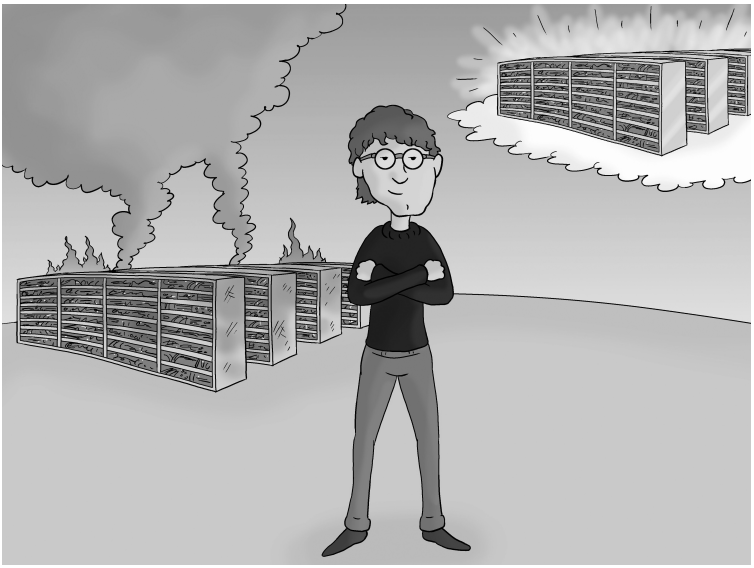
To learn more visit
www.veeam.com

Conversational Disaster Recovery as a Service

By Brien Posey

With foreword by Jason Buffington

© 2022 Conversational Geek



ConversationalGeek®

Conversational Disaster Recovery as a Service

Published by Conversational Geek® Inc.

www.conversationalgeek.com

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

Trademarks

Conversational Geek, the Conversational Geek logo, and J. the Geek are trademarks of Conversational Geek®. All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. We cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or programs accompanying it.

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author:	Brien Posey
Project/Copy Editor:	Nick Cavalancia
Content Reviewer(s):	Jason Buffington
	Denise Jongenelen
	Laura Vanassche

Note from the Author

Hi, I'm Brien. For those of you who don't know me (or know my work), I am a long-time Conversational Geek author, and 19-time Microsoft MVP. In addition to my ongoing work in IT, I have also spent the past several years training to be a commercial astronaut. IT and astronautics are definitely an odd combination. Thankfully, my friends at Conversational Geek have embraced my unorthodox (dare I say eccentric) career choices and have allowed me to author books on subjects ranging from AWS to real-life rocket science.

In this book, I wanted to write about Disaster Recovery as a Service (DRaaS). Not all that long ago, DRaaS was super-expensive and you practically needed a PhD. in computer science to make it work. Today, though, the cloud has made DRaaS affordable and accessible for nearly everyone. Even so, there are a number of things to think about when implementing a disaster recovery solution. That's what this book is all about. I'm going to share with you some of the things that you need to be thinking about as you evaluate the various DRaaS offerings that are available.

Oh, and one more thing… this book is not intended to be a vendor product pitch. My goal here is to take a vendor-neutral approach to the subject at hand.

Brien M. Posey

The “Conversational” Method

We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so that it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend, and even the know-it-all Best Buy geek on a level playing field.

“Geek in the Mirror” Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these “geek in the mirror” boxes are not to be skipped.

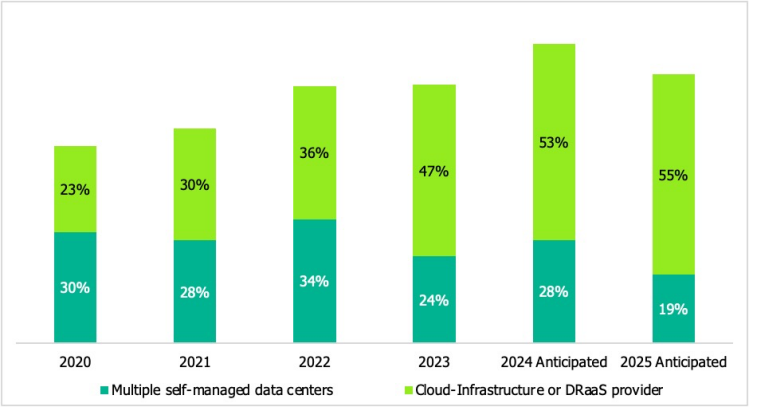
Greetings. Within these boxes I can share just about anything on the subject at hand.

Read ’em!

Foreword: The Future of Disaster Recovery is "Cloudy"

In 2023, Veeam® released what is the largest global survey[1] to date, asking 4,200 unbiased IT and business decision makers to capture their data management challenges and successes, including data protection drivers and strategies. We discovered some incredible insights and trends, but one thing is very clear: The future of disaster recovery is cloudy.

One survey question focused on identifying organizations' current and future business continuity and disaster recovery (BC/DR) strategies. The goal of this question was to find out whether they would continue to manage their own secondary BC/DR sites or utilize cloud-hosted infrastructure — including either self-managed Infrastructure as-a-Service (IaaS) or a managed service provider who delivers Disaster Recovery as-a-Service (DRaaS).



There are two key takeaways here:

First, there are still plenty of organizations maintaining multiple data centers for backup and disaster recovery (DR), with IT architecture designed to protect each location (i.e., an east coast data center protecting one on the west coast and vice

versa) — though there is consistent intent to reduce the need for multi-datacenters:

- In 2022, 34% managed their own secondary datacenters, but planned to reduce to 28%

- In 2023, 24% managed their own secondary datacenters, but planned to reduce to 19%

Should secondary datacenters go to 0%? No. There are some great scenarios empowered by that architecture, but the growth (and shifts) in BC/DR unmistakably come from cloud-powered disaster recovery. From 2020 to 2023, actual usage of cloud-hosted infrastructure doubled from 23% to 47%, with even more expecting to use DRaaS or cloud infrastructure for DR by 2025.

But what does this really mean, and why? We'll dig deeper later in this book, but there are consistently two universal appeals to DRaaS:

- Elastic infrastructure: Instead of building and maintaining secondary (and expensive) physical infrastructures in another location, cloud-hosted infrastructures can spin up whenever you need them, and they will cost you far less when you don't.

- Specialized expertise: Most organizations have IT professionals who understand and maintain backups of their data, but the skills necessary to ensure that a company is prepared for and successful during a data disaster are very different. DRaaS providers are the true technical experts in orchestrated workflows, network redirection, storage management, rapid provisioning and testing/reporting methodologies.

Before I hand it over to Brien, there's one more key industry highlight to share regarding BC/DR preparedness. Statistically, organizations that self-manage their BC/DR infrastructures have reported testing for disaster preparedness either annually or semi-annually. The reason for this comes from the challenge of traditional outage windows, "declared" disaster tests, cut overs, etc.

Instead, companies who leverage DRaaS reported testing at least part of their infrastructure (i.e., one set of servers) every five weeks. Why? DRaaS makes it easier because it's:

- Cheap, due to its elastic infrastructure
- Easy, due to newer orchestration methods
- Unencumbered, due to "sandbox" or other noninvasive testing frameworks
- Timely, since IT could run tests during the week and completely on a whim

A fundamental truth of disaster recovery is that the more you test, the more likely it is that you'll be able to recover your data when you really need to. This is another major advantage to DRaaS that will be covered later. In fact, Brien kicks things off with a story from his early DR testing days you won't want to miss.

This e-book is designed in a conversational way to layout the basics of cloud-powered disaster recovery and the significant advantages that DRaaS offers businesses who are looking to modernize their BC/DR strategy.

Jason Buffington (@JBuff) has been working in data protection for 32 years, is VP of Market Strategy within the Office of the CTO at Veeam, and formerly the Principal Analyst for Data Protection at the Enterprise Strategy Group (ESG).

Disaster Recovery, Powered by the Cloud

I spent the early part of my IT career working for a large insurance company. One thing that sticks out in my mind when remembering that gig was the day our boss told us we'd be doing a disaster recovery test. At the time, I was brand new to enterprise IT and had never heard of a disaster recovery test.

Ultimately, the test involved loading backup tapes onto an airplane and flying them (along with half of the IT staff) to a data center on the other side of the country. The goal was to verify that the tapes could be restored onto standby systems in the backup data center, after which we'd run a test that

involved temporarily transitioning all the organization's IT activities to a standby data center.

The thing that stood out to me about this exercise was how unbelievably expensive it must have been. Even today, I can't imagine the costs involved in building a standby data center just to have it sit idle in case there was a disaster — never mind the cost of chartering a private jet for half of the IT staff to the backup site.

After the exercise was over, I realized two things. Firstly, our organization viewed disaster recovery as being so important that it accepted the enormous costs involved in building, maintaining and testing a disaster recovery infrastructure. Second, only a huge corporation would have the financial resources and the IT expertise to do something like that. That type of disaster recovery preparedness would have been completely out of reach for a smaller business.

Industry analysts can't seem to agree on the hourly cost of downtime. That's probably because every business is different, so costs are also different from one business to another. Some have estimated the cost of downtime to be over half a million dollars per hour! (goto.cg/3GxZp4l)

Today, things are different. Disaster recovery was once so absurdly expensive and difficult that only a huge company could do it. Now, the cloud allows almost any organization to put a disaster recovery solution into place.

What's more is that today's low-cost disaster recovery solutions are far superior to the multi-million-dollar disaster recovery solutions that existed back then.

Think about it for a moment. Back then, the only viable option for disaster recovery was to put the backup tapes onto an airplane, fly to the other side of the country, restore the backup tapes and perform some IT voodoo magic to transition everything over to the new environment. Imagine the amount of downtime IT operations needed to do that — never mind that for the operation to succeed, the tapes would have to survive whatever disaster prompted the failover in the first place.

In contrast, today's disaster recovery solutions allow an organization's IT operations to failover to the cloud almost instantly. This is referred to as Disaster Recovery as a Service (DRaaS). Once a failover happens, the organization can leave everything running in the cloud for as long as they want. Once the disaster is over, workloads can easily be brought back inhouse, or they can be permanently migrated to the cloud.

There are huge advantages to DRaaS that more and more companies are starting to realize, not just enterprises. Before we dig into that, let's start with some of the basics of cloud-powered disaster recovery.

Disaster recovery and DRaaS

As you may have gathered, disaster recovery is different from traditional backups. While backups focus on creating a restorable copy of an organization's data, disaster recovery takes backup and recovery to the next level by allowing an organization to transition workloads to an alternate location in the event of a disaster.

As I previously illustrated, disaster recovery has traditionally been expensive and extraordinarily difficult to implement. This is where Disaster Recovery as a Service comes into play. DRaaS is essentially a subscription-based disaster recovery service. In it, the service provider makes cloud-based disaster recovery available to its subscribers at a reasonable cost. In doing so, the

provider leverages automation as a way of taking complexity out of the disaster recovery process. I'll go more into detail about this later.

For now, let's say that having a provider who is able to use orchestration to automate complex disaster recovery tasks is a big deal. Not only does this make life easier for the subscriber's IT staff, but automation also reduces the potential for human error and reduces the amount of time required to recover the workload. In the unlikely event that something goes wrong during the failover process, a good DRaaS provider has the business and IT expertise required to help if needed.

If you're already working with a service provider for your backup (i.e., Backup as a Service), think of DRaaS as a subset of an overall BaaS strategy. BaaS might get your data out of the building, while DRaaS presumes that you'll take that survivable data and re-mount it elsewhere. Instead of restoring your data, you'll resume services by simply powering up the replicated servers (instead of data sets) within a cloud host. It sounds too good to be true, so why wouldn't you do that?

Well, it comes with its own complexities — but it's absolutely achievable with the right partner and the right technologies.

Before I move on, there's one last thing I want to mention. There is often a perception that disaster recovery and DRaaS exist solely as a last line of defense, should something truly catastrophic happen. After all, most material written about disaster recovery focuses on hurricanes, volcanic eruptions and nuclear blasts.

In reality, disaster recovery isn't something to use only if there's a smoking crater where your data center used to be. It can also be used for something as simple as a server outage or an accidental file deletion. Because today's DRaaS solutions are inexpensive, fast and easy to use, an organization can failover workloads to the cloud on an as-needed basis. They can just as

easily fail them back over to their original location once the situation is resolved.

Common IT data protection challenges

As I previously explained, the cloud has been a game changer when it comes to disaster recovery. What used to require untold millions of dollars and a tremendous amount of IT expertise is now within the reach of almost anyone. The fact that huge corporations used to spend fortunes on disaster recovery operations is an indicator of just how important it is to have solid disaster recovery capabilities. Beyond that, a good disaster recovery solution can help an organization effectively deal with some of the biggest challenges its IT staff faces on a day-to-day basis. I'll give you a few examples.

First, consider what happened in 2020. Most of the world's office workers abruptly transitioned to working almost exclusively from home. As it stands now, it seems as though the work-from-home trend will go on for quite some time (if not indefinitely). Forrester found in a 2021 survey of U.S. and European business owners that only 30% of companies will embrace a full return-to-office model post-pandemic[1].

The abrupt transition to remote work was a huge challenge for IT departments everywhere. Thankfully, IT rose to the occasion and got the job done. I can't imagine how much worse it would've been had it not been for all the hard-working IT professionals.

Even though enabling and supporting a remote workforce was the first order of business, there were other obstacles. Just because everyone was suddenly working from home did not

---

1. Source: https://go.forrester.com/press-newsroom/forrester-only-30-of-companies-will-embrace-a-full-return-to-office-model-post-pandemic/

mean that service level agreements (SLAs) became irrelevant. Organizations still expected their SLAs to be honored despite the adverse situation.

IT pros quickly discovered that SLAs are far more difficult to maintain when everyone is working remotely and that having a solid disaster recovery plan made it easier to maintain your SLAs.

IT already handles a lot

As we all know, IT budgets seem to get smaller each year. One way organizations cope with these ever-shrinking IT budgets is by taking advantage of attrition. In other words, when members of the IT staff resign, they are simply not replaced. This helps save money, but it puts the remaining IT staff in a bad position.

Being short-staffed is always challenging, regardless of profession. We've all been to understaffed restaurants and seen how difficult it is for the waitstaff to keep up.

IT suffers from these same challenges, but there is one thing that makes IT unique in this case: IT is so dense and so complicated, it's impossible for individual IT professionals to have expertise in every area (believe me, I've tried). As such, there aren't many IT generalists left in the world; most IT professionals specialize in certain areas. If organizations limit the headcount of their IT staff, there will inevitably be certain areas of the organization lacking in expertise.

The 2023 Data Protection survey that Jason referenced in his foreword fully supports this — freeing up internal resources to focus on modernization was named a top strategic priority.

One way an organization can get around the problem of having insufficient expertise in certain areas is to adopt managed cloud services. This is especially true for disaster recovery. Disaster recovery is far more complex than most people realize. An organization would do well to outsource its disaster recovery efforts to a cloud service provider that has the necessary expertise.

Making the shift to innovation

It's been said that working in IT is a bit like herding cats. In all the organizations that I've ever worked, chaos was the order of the day, and the IT staff's time was always spent on keeping things running and dealing with issues as they come up.

I've often said that the true purpose of IT is to use technology to solve business problems. So, if an IT department is focused on dealing with day-to-day issues and doesn't have the time to do anything else, then IT isn't living up to its true purpose.

Outsourcing disaster recovery operations to a DRaaS cloud provider is one way of freeing up some of the IT staff's time, making it possible for them to focus on innovation and on strategic projects that will ultimately help grow the business.

Modernizing your infrastructure

Another problem IT departments commonly face is that of outdated infrastructure. This problem is connected to ever-shrinking IT budgets. After all, it's tough to do a hardware refresh if you don't have the money for new hardware.

Being understaffed can also contribute to having an outdated infrastructure. I am currently working through a hardware refresh in my own organization. Even so, I stay so busy that it's hard to find time to complete the process. At the moment, there are boxes of new hardware gathering dust in my office as I wait for an opportunity to install it.

If you find yourself in a situation where you simply don't have the budget to replace aging hardware, then moving certain workloads to the cloud can help. After all, cloud providers are responsible for maintaining their own infrastructure. This means that you don't have to worry about the cost of new hardware or finding the time to deploy it.

Often overlooked, however, is that disaster recovery hardware must be at least as good as the hardware that workloads are currently running on. Remember, end users and customers don't care that you've experienced a failure; they expect workloads to run as they always have. This means that using subpar hardware for disaster recovery purposes isn't a good option.

This simple concept is a big part of why disaster recovery operations have often been cost-prohibitive. It doesn't make financial sense to purchase high-end hardware just to have it sitting idle on the off chance that it will one day be needed. Since hardware is usually refreshed every three to five years, there is a realistic chance that some disaster recovery hardware will never be used.

This is another reason why it makes so much sense to use the cloud for disaster recovery. Since cloud providers supply the hardware you need, you can rest assured that your hardware

will be adequate to handle your disaster recovery operations. When hardware begins to age, it's the cloud provider — not you — paying for the upgrade.

What should you look for in a DRaaS solution?

As you evaluate DRaaS solutions, you will discover that available solutions vary greatly in terms of features, costs and capability. I'll talk about some key things you need to look for in a moment. For now, I want to discuss three things that are often overlooked when it comes to choosing a DRaaS solution. These include expertise, speed and ease of use.

Expertise

One of the first things to consider when choosing a DRaaS solution is service provider expertise. Disaster recovery is a lot more complicated than most people realize (I'll talk more about that a little bit later).

For now, the important thing to know is that disaster recovery service providers need to have the expertise that's required to make sure that their solution is 100% reliable. While you may be able to save a few bucks by going with a start-up or fly-by-night provider, cutting corners can come back to bite you.

Another way that expertise comes into the picture is in the form of support. If you end up in a situation where you've experienced a failure and something has gone wrong with your disaster recovery solution, you need the assurance that technical support is able to resolve the issue quickly. Remember, not only is downtime extraordinarily expensive, but a disaster recovery failure could cost you your job. This is all the more reason to make sure that you choose a provider that has the expertise to help you implement disaster recovery capabilities in the right way and deal with any situation that may arise.

Speed

The need for speed is a no-brainer, but it's still easy to overlook. As previously mentioned, downtime is ridiculously expensive. The faster you're able to transition to a disaster recovery environment, the less a failure will cost you. To put this another way, speed saves you money.

In addition, speed isn't the only failover that matters — time to value also is important. In other words, how quickly will you be able to see a return on your DRaaS investment?

Other factors to consider are how swiftly you're able to get started with your DRaaS strategy and how you can scale your disaster recovery infrastructure as your organization grows. In the past, it took months to design and implement a disaster recovery plan. Today, however, DRaaS providers can help organizations get started right away.

Customer ease of use

Disaster recovery is a simple concept at its core. The whole idea is that if a failure were to occur within an organization's primary environment, the organization can failover to a secondary environment able to take over as if nothing ever happened. That said, like with so many other things in the world of IT, the devil is in the details.

As simple as DR may be on paper, it is a surprisingly complicated thing to implement. There are a million things going on behind the scenes in order to make disaster recovery possible. Let me give you just one example of something that needs to happen.

Suppose for a moment that an organization experiences a failure of a critical application server and they transition the workload to their disaster recovery environment. Let's also suppose the application consists of a front-end server and a back-end database server.

Because this application runs in a new location, both the front-end server and the database server are required to run in a different subnet. This means that both servers need to be assigned new IP addresses. This also means that the DNS servers on the private network have to be updated so that the servers can once again resolve each other's IP addresses. This is so that any resources that continue to exist in the organization's primary location can locate the application once it's been moved.

Still with me? If the application happens to be public facing, then the authoritative DNS server will also need to be updated so clients can be redirected to the new application server. On top of all of that, there are probably going to be a number of firewall rules that need to be modified.

In other words:

- The front-end server and database server run in a different subnet and are assigned new IP addresses
- DNS servers on the private network are updated to resolve each server's IP address
- For public-facing applications, the authoritative DNS server is updated and clients are redirected to the new application server
- Firewall rules also must be modified

This is just one example of a critical task that must be performed as a part of an application failover. There are plenty of other things that also need to happen. This is why ease of use is so important. Your disaster recovery solution needs to be able to handle these types of granular tasks for you, such that everything's working properly in the disaster recovery site. More importantly, the same automation that makes a disaster

recovery solution easy to use also helps reduce the amount of downtime that comes from a failure — which, in turn, helps reduce costs.

Even if you put all of this aside, there is one more reason why ease of use is important. If you happen to experience a failure and need to failover to a disaster recovery site, you don't want to have to guess about how to perform the failover. The software should be intuitive enough that you can initiate the failover (if it isn't automatic) without a lot of effort.

Other key considerations

Speed, expertise and ease of use are all major considerations when it comes to selecting a DRaaS provider. There are, of course, other things to look for.

One of the more obvious additional considerations is cost. Clearly, any solution that you choose must fit within your budget. As you evaluate the cost, however, it's important that you look at more than just the cost of the DRaaS subscription. You will also need to consider costs like cloud storage and data egress fees (though your service provider can help you navigate these nuances).

In my decades of working with customers and vendors, it's also key that a particular DRaaS provider aligns with your operational needs. For example, if all your workloads are running on Windows, then it wouldn't make sense to use a provider who focuses on Linux. This is an important consideration to keep in mind as you evaluate DRaaS solutions.

Of course, most organizations today use a combination of different platforms. An organization might have a combination of Windows and Linux workloads running on top of VMware, Hyper-V and Nutanix. As such, any DRaaS solution you implement must be flexible enough to work with the various platforms you are using.

If your organization is subject to any type of governmental regulations, then regulatory requirements and compliance should be at the top of your mind. You will need to make sure that your chosen DRaaS provider is able to comply with any applicable regulations across different industries and geographic regions.

It's also important to think about scalability and reliability. For a DRaaS solution to work, existing data and applications must be replicated to the cloud. The problem arises in that the replication engine can become a choke point — which is especially true if the data has a high change rate or if the organization continues adding additional workloads. You may reach the point where the existing cloud gateway is unable to keep up with the demand.

Likewise, the cloud gateway itself can become a single point of failure. If the cloud gateway were to fail, then your data is no longer being replicated to the cloud, thus undermining your entire disaster recovery plan.

Given the critical role that the cloud gateway performs, it is important to make sure that your DRaaS provider supports the use of multiple cloud gateways. At the very least, you should have a redundant gateway to help protect against outages. However, it’s also important to be able to distribute data transfer operations across multiple gateways to ensure that data is uploaded to the cloud in accordance with your SLAs. And as your IT footprint increases, you should be able to seamlessly add more cloud gateways to service the additional demand.

Finally, it’s important to think about what a DRaaS service can do to keep your data safe. This might seem like an odd thing to think about, considering protection is whole point of DRaaS. Even so, you should look beyond failover and consider the data itself.

Suppose for a moment that your organization were to suffer a ransomware attack. A DRaaS solution probably isn't going to be able to tell the difference between data encrypted by you and data encrypted by ransomware. As such, it will dutifully replicate your now-encrypted data to the cloud, overwriting the good copy of your data in the process. Ideally, however, your DRaaS provider should be taking advantage of cloud-based immutable object storage, which would make it far easier to recover from a ransomware attack.

Similarly, a good DRaaS solution should give you other options for protecting your data. For example, since outbound data must pass through a cloud gateway, a provider might give you the option of writing a copy of the data to disk or tape for safe keeping.

The Big Takeaways

IT professionals have a tough job. On one hand, budgets are getting smaller every year. At the same time, business leaders have ever-increasing expectations for their IT departments. This puts IT professionals in a difficult position. They are continuously being told to do more with less, with no room for failure.

As a best practice, organizations should look for a DRaaS provider that understands all the nuances and unique requirements that a business has when it comes to a disaster recovery solution. At the same time, the provider needs to take the extra step of making things as easy on IT professionals as possible. After all, the idea is to proactively improve your organization's disaster recovery strategy while also making your own life easier in the process. That way, you can focus less on data protection and disaster recovery, and free up time to help your organization with transformative initiatives that will help them stay competitive.

A DRaaS solution should be:

- Easy to implement and easy to use, relying on orchestration to automate otherwise complex, manual tasks
- Fast and efficient enough to protect against small outages or file-level deletions, not just catastrophic data-center-level events
- Scalable and capable of protecting all your virtual machines (VMs), databases, storage systems and applications, no matter where they reside.

- Able to “just work.” You should be able to fail over production or test data without complex administrative steps or specialized backup technology

- Offered by a DRaaS provider with the expertise and industry know-how needed to maintain your SLAs and regulatory compliance

- Able to provide the visibility you need into your DRaaS environment without having to manage multiple tools and systems, with easy reporting for your auditors and regulators

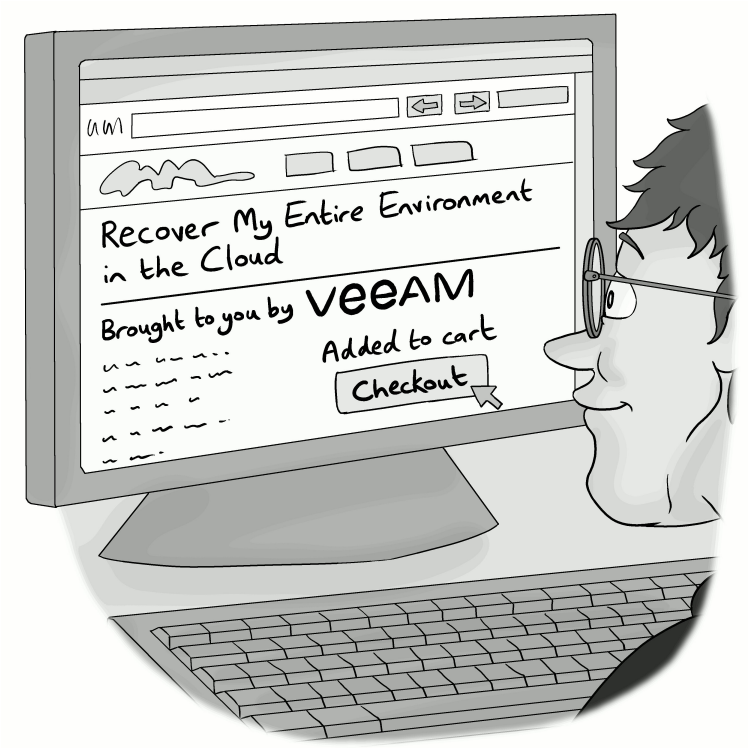
- Cost effective and able to quickly deliver a return on investment by dramatically reducing your recovery times and avoiding costly hardware expenditures

- Scalable and offer sufficient redundancy to eliminate any single points of failure

- Able to look for additional ways to protect your data, such as allowing tape backup or giving you the option of using immutable storage

Most importantly, a DRaaS solution should provide you with the assurance you need to know your organization can and will survive a data disaster of any size and any kind. And that’s the point of DRaaS; service providers are here to lessen that load and make your IT department the champion of the business.

DRaaS, Powered by Veeam



We've looked at the basics of cloud-powered disaster recovery, common challenges faced by IT organizations big and small, the ways in which DRaaS can solve for them and considerations to keep in mind as you evaluate a DRaaS solution and provider.

The trickiest part can be actually finding and evaluating a solution that does all that — and the right partner to fit your business and IT needs.

For over 10 years, Veeam has been an industry leader at powering BaaS and DRaaS. More than 450,000 organizations

around the world currently trust their critical data to be protected by Veeam solutions, including 81% of the Fortune 500. Veeam is also consistently named a top data protection leader by Gartner and IDC, among other industry analysts.

Veeam provides a single platform for modernizing backup, accelerating hybrid cloud and securing your data.

This platform can be integrated easily into any environment as it is software defined and hardware agnostic. This offers simple, flexible and reliable backup and recovery.

A good way to show what this means in practice is to look at how Veeam can help meet each stage of a BaaS and DRaaS strategy.

Evolution phase one — Storage (survivable data)

For some organizations, cloud-powered data protection is as simple as utilizing cloud-hosted storage as an off-site repository. For that, Veeam offers at least two options:

Self-managed DRaaS: Users can easily achieve longer-term data retention in object storage with Veeam Cloud Tier (which is built into the company's flagship backup and recovery product, Veeam Backup & Replication ™), as well as leverage direct-to-object storage for enhanced performance.

Service-managed: Veeam Backup & Recovery also offers a feature called Veeam Cloud Connect, which makes backup and recovery easy, whether it's to, from or within the cloud. Cloud-powered backup and recovery can be complex to set up, but Veeam Cloud Connect enables you to begin backing up your data to the cloud in just a few clicks. Also, Veeam's global network of cloud and managed service partners can provide additional services, such as cloud hosting, remote management, expertise, support and more.

Evolution phase two — Backup (operational recoverability)

Once you know your data is protected in the case of a data disaster, the next step is to optimize your processes and improve your capabilities. This is where you start to consume backup capabilities "as a service", which to most folks means a few key elements:

- Paid for "as you go" (based on what service features you use), instead of the upfront purchases of hardware and software

- Faster time to value by not requiring your own IT staff to assemble, deploy and configure the backup servers and storage repositories

- Superior reliability of backups and recoveries. This is in large part due to the expertise of the service provider, who is trained by the backup software vendor as experts, yet has contextual empathy with each customer consuming their services

When you combine these three tenants, you get several consumption models:

Remote management: For many organizations, service level agreements, regulatory requirements, overall IT architecture and corporate culture can collectively require that backups must be operated within IT premises. And yet, there are value-add resellers and distributors who offer MoBaaS (Management of Backups as-a-Service) to remotely monitor and operate what is otherwise an on-premises backup solution. If MoBaaS isn't a term you are familiar with, then just consider it the outsourcing of the backup manager role. In most cases, the pay-as-you-go model (with the backup hardware/software often leased to the client) has fast time to value and reliable management due to dedicated expertise.

Traditional BaaS: For many, this means that the backup servers are running as services, which could be either a SaaS-architected backup service or cloud-hosted (IaaS) backup server. Either way, these backup capabilities come without IT teams building and maintaining on-premises backup hardware and software, and include some level of monitoring the health of the backup servers and storage repositories.

Managed BaaS: Managed BaaS builds on top of traditional BaaS, where the organization's IT professionals are still responsible for daily backup jobs, restore requests, architecture evolution, performance tuning and documentation. Managed BaaS outsources those expertise-centric and repetitive functions to the service provider as well. This can vary from simple operations center or help desk customer services to a full white-glove extension of the IT team's turnkey service.

In Veeam's case, they partner with a range of Veeam resellers, accredited service providers, and cloud and managed service providers that deliver each of these options.

Evolution phase three — Disaster recovery (resiliency of business processes based on rapidly recoverable or durable IT delivery)

As a model, backup is focused on your data. Specifically, it's focused on the retention of previous versions of your data. Your backup tools use (or ought to use) backups, snapshots and replication in tandem with one another. But to "recover" using backups, snapshots or replicas means that you need to first restore the data.

In contrast, disaster recovery is usually focused on IT service delivery, where the focus of recovery isn't on restoring previous versions of data. Since it is failing over servers, it allows the continuation of business processes that rely on those IT services and servers. To be clear, preservation of data

is a foundational and critical part of BC/DR initiatives, but the mindset is much larger. Equally as important, the expertise necessary to be successful with BC/DR is broader than the skills necessary to back up or restore data.

There are multiple DR options available with Veeam:

Self-managed DR: Many enterprises and larger commercial organizations operate multiple data centers and have IT teams at each of them. If you have BC/DR expertise as well, you can combine Veeam Backup & Replication with both Veeam ONE™ for monitoring and Veeam Disaster Recovery Orchestrator for workflows, testing and documentation.

Architected DR: Even among large organizations, IT teams often lack BC/DR expertise in business-process planning and IT architects who understand how to re-host and resume complex applications and systems at an alternate IT site or service. The solution might be self-managed, but it requires upfront and ongoing supplemental expertise. This is a key area of focus for Veeam Accredited Service Partners with specific skills in BC/DR. It is something that every self-managed enterprise looking for better BC/DR should consider.

Disaster Recovery as-a-Service (DRaaS): Due to its breadth and flexibility, this can potentially be the ultimate service for recovering from almost any IT crisis. DRaaS in its highest form combines several of the above-described tenants. These include:

- Backup and replication services (including snapshot-based and continuous data protection) that are provided to a cloud host, paid for by consumption, and operated and monitored by experts within the service provider

- As an off-site provider, insurance of not only data survivability (evolution one) and operational recovery

(evolution two), but also the ability to recover within the provider's environment without first restoring data back to the on-premises source

- BC/DR expertise in both business process mapping and processes, along with IT expertise in protecting and failing over servers and services from a remote location

With high expertise requirements, alongside resilient infrastructure that is agile enough to resume IT services, not every BaaS solution is a DRaaS solution, nor is every BaaS provider a DRaaS provider

Veeam combines backups, snapshots and replication for physical, virtual and cloud-hosted workloads, while providing options for great outcomes that could be self-managed, cloud-powered or truly cloud-delivered (i.e., DRaaS).

Data center | Endpoints | SaaS | Cloud

Veeam powers a global network of cloud and managed service providers to deliver expert-built and managed Backup as a Service (BaaS) and Disaster Recovery as a Service (DRaaS) to organizations of all sizes. Powered by the Veeam Data Platform, you can rest assured your data is protected and resilient, no matter where it resides.

FIND A PARTNER

LEARN MORE

©2022 Veeam® Software. All rights reserved. All trademarks are the property of their respective owners.

Quickly become conversational about Disaster Recovery as a Service (DRaaS)

Is your production data ready for when disaster strikes? Building and maintaining a DIY Disaster Recovery solution has traditionally been seen as time-consuming and costly. Partnering with a service provider that offers Disaster Recovery as a Service, or DRaaS, takes the management and complexity off of your hands at a reasonable cost. Allowing you to focus on innovative projects to grow your business. In this book we'll explain why having a provider with the expertise to implement and manage a complex disaster recovery solution is a huge benefit to organizations.

About Brien Posey

Brien Posey is a 19-time Microsoft MVP, a published author and conference speaker with 20+ years of IT experience, and a Commercial Scientist Astronaut candidate.

ConversationalGeek®

For more books on topics geeks love visit

conversationalgeek.com