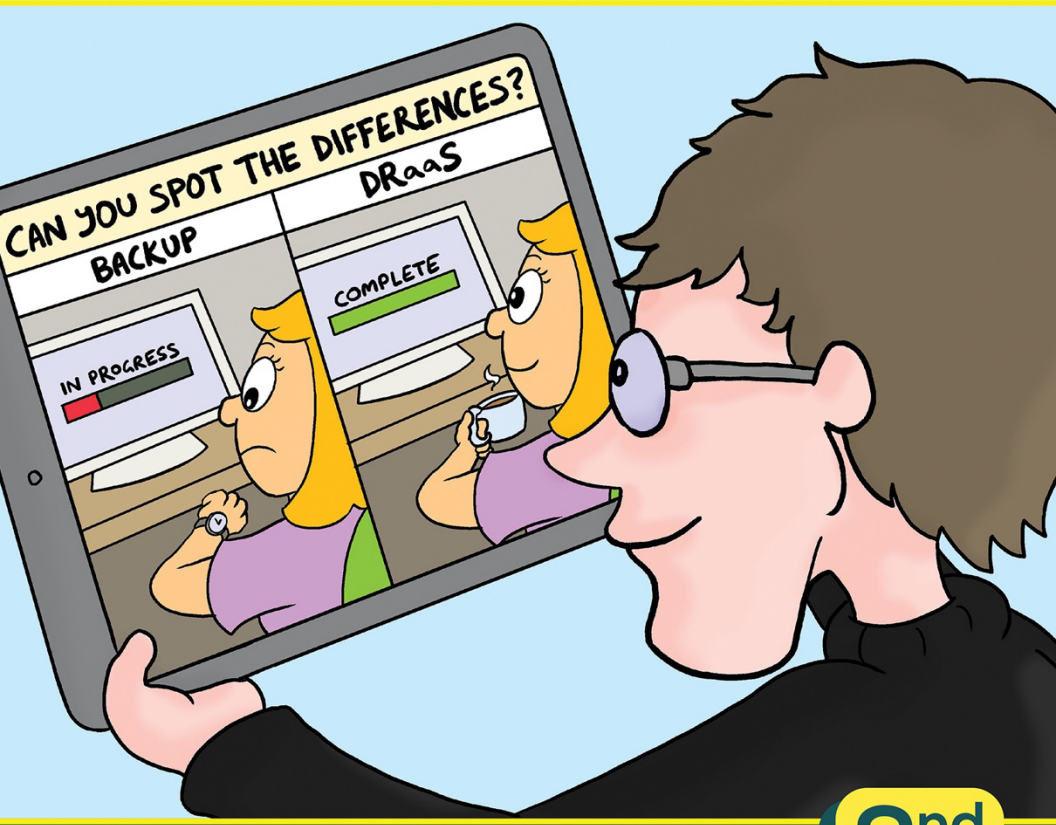
ConversationalGeek®

Conversational
Backup is not DRaaS

By Nick Cavalancia (Microsoft MVP)



2nd Edition

In this book, you will learn:

- The key differences between Backup and DRaaS
- What to expect from Backup and DRaaS solutions
- How to develop a proper data protection strategy

Sponsored by CyberFortress

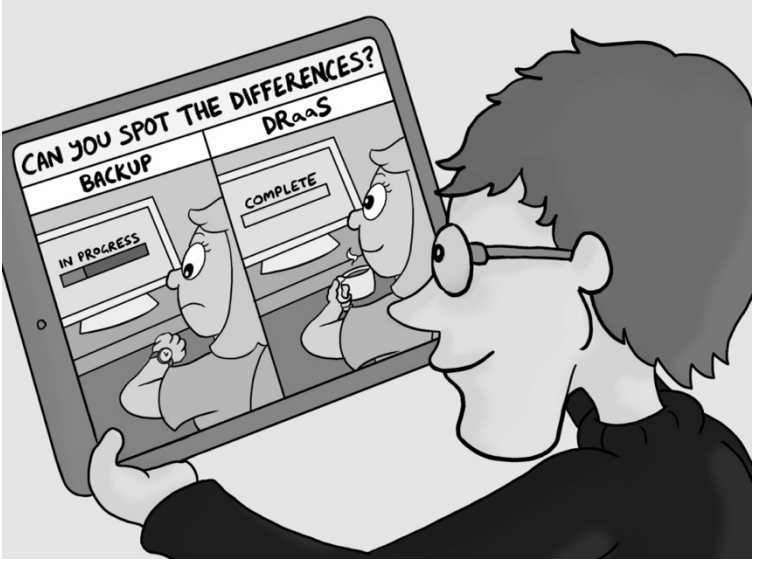
CyberFortress is a global company that makes it simple to fully backup and rapidly recover all lost or stolen data to prevent damage and disruption to organizations of all sizes. We provide highly available and secure cloud data protection Disaster Recovery (DRaaS) and Backup (BaaS) solutions built on market leading technology from Veeam.

Data is stored in secure, geo-redundant facilities meeting our diverse customer's SOC 2, ISO 27001, PCI-DSS, and HIPAA compliance needs. Our suite of solutions enables CyberFortress' data recovery specialists to create a custom, comprehensive solution for each customer. Whenever a customer needs data recovery, they can rely upon CyberFortress for live, personalized support from a credentialed specialist 24x7x365.

For more details visit
www.cyberfortress.com

Conversational Backup is not DRaaS

By Nick Cavalancia



ConversationalGeek®

Conversational Backup is not DRaaS

Published by Conversational Geek® Inc.

www.conversationalgeek.com

Trademarks

Warning and Disclaimer

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:	Nick Cavalancia
Project/Copy Editor:	Hope Crocker
Content Reviewer(s):	Becky Cook
	Nick Natale

Note from the Author

The journey for every organization around putting proper data protection in place always starts with backups to maintain copies of critical datasets for when disaster strikes. But making copies for the sake of having them "just in case" feels like it's more a technical decision than a business one.

The business has its own needs around the availability of all of its data, applications, and systems. This, in turn, should influence what the technical requirements are for IT to meet around what to backup, how often, and using what methodology. It should also influence the technical implementation decisions that establish constraints around time, staffing, expertise, and cost when it comes time to actually recover.

In this eBook, I'm going to make the case that Backups and DRaaS are most definitely not the same thing. And, while my intent is not necessarily to persuade you to shift to DRaaS, I do want to actively educate you on why the two are vastly different and provide distinct recovery outcomes because of their unique approaches to protecting data.

And, if it turns out you come to realize DRaaS may be a better option, I'm happy that you've elevated your thinking about how to approach data protection.

Nick Cavalancia

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!

Backup vs. DRaaS?

"Heads, it's Backups, tails it's DRaaS!"

There isn't a more critical part of IT today than protecting your data, systems, and applications. The expectation of your business now includes always being available to customers, partners, and employees. Along with the threat of cyberattack, natural disaster, and human error, you simply can't afford *not* to be operational as close to 100% of the time as is possible.

Whether you're a cloud-first organization, running solely on-premises, or doing something hybrid (which I suspect most of you are), the

concept of maintaining an appropriate level of business continuity is a must.

Should there be a loss of any magnitude that impacts operations, every workload, application, system, and piece of data needs to be able to be recovered to a working state quickly and accurately. But it's more than just recovering resources and data; it's about bringing the business back into an operational state.

Backup has been around for decades and its core concepts remain the same even today, despite advances in backup methods, storage mediums, and use of virtualization. Modern approaches such as Disaster Recovery as a Service (DRaaS) add on secondary sites, replication, and assistance to augment backups. Many organizations don't see the value in DRaaS and even go as far as to think they are "pretty much" the same. I'm a big believer in a mature disaster recovery approach over that of traditional backups, so I'm going to try to make the case in this eBook that the two *definitely* are not the same… and that you should be thinking seriously about DRaaS.

To do this, I'm going to discuss the risks businesses face today where recovering some or all of your operations is necessary, and compare Backup and DRaaS from a few different perspectives, including one of the most common modern-day disaster scenarios – *ransomware*.

I'd like to first level set why you even need backups or DRaaS in the first place, to establish the business reasons why the choice is an important one.

The Risk to Business Continuity

That expectation of always being operational I mentioned before means business continuity needs to be a priority (if it isn't already). And that means having a clear understanding of where the risks are that pose a threat to continuous operations. If you're not including a risk assessment of your business continuity plans, you're doing the

organization a disservice, as nearly two-thirds (65%) of organizations feel like the level of business continuity risk is actually *increasing*[1].

There are a number of risks to the business that are clear and present and should be considered when coming up with a proper strategy to ensure the business stays operational.

- Cyber Attack – This one tops the list of risks[1] because of the massive growth in the frequency and number of ransomware attacks. With an average of 45% of production data affected during a ransomware attack[2], an average downtime post-attack of 3 weeks[2], and an average overall remediation cost of $4.45 million[3], it's evident that this is likely the most material risk to your business continuity.

- Business Complexity – As you adopt new technology, engage in M&A activity, shift your focus to the cloud, and even take on a multi-cloud approach, the larger the impact of a business disruption becomes and the less likely it is that you'll easily be able to restore affected parts of the business back into an operational state quickly.

- Reliance on Third Parties – The adoption of SaaS, PaaS, and IaaS has traditionally come with the catch that your organization loses some level of control. And yet, should there be a business disruption, even those parts of operations may need to be recovered, reconfigured, etc. Only half of organizations have a formal process for validating the business continuity readiness of their third-party partners, suppliers, and service providers[1].

---

[1] Forrester, *The State of Business Continuity Preparedness* (2023)

[2] Veeam, *Ransomware Trends Report* (2023)

[3] IBM, *Cost of a Data Breach Report* (2022)

- The Usual "Disasters" – While not as in the forefront of your mind these days, the disruptions we traditionally called "disasters" like weather, fire, human error, etc. all still need to be considered as potential risks when determining your continuity strategy.

While you may think an actual disaster event will never happen, but 1 in 4 organizations have had to invoke their Business Continuity Plan more than five times in the last five years! [1]

Despite these risks, most organizations simply aren't ready should some kind of disruption event occur. More than one-quarter (27%) of organizations with business continuity plans *never* perform a full simulation recovery of some or all of their environment[1], with more than three-quarters (76%) only performing tabletop walkthroughs once a year[1].

So, given the fact that you need to have a strategy for how you're going to recover *when* one of these disruption scenarios happens, the discussion needs to turn to answer the question of what data protection model is going to best serve the needs of your organization.

Based on the title of this eBook, it's probably safe to assume that many of you are focusing on maintaining backups of everything from your critical workloads to the entire organization, thinking with proper backups you should be able to easily restore anything that is unavailable post-disruption.

But advancements in methodology and technology have resulted in the availability of DRaaS and, given the risk your business faces by not being operational, I'm going to spend some time comparing traditional backup with DRaaS in an effort to aid you in determining whether backup will continue to meet your business needs or if you need to be looking at something closer to DRaaS.

Comparing Backup and DRaaS

The need to resume operations as quickly as possible after a disruptive event requires having the right method of data protection and, eventually, recovery of data, systems, and applications when an event *does* occur. The concept of backups has been around for decades, while DRaaS has been significantly evolving over the past five years, causing many organizations to take sides – one perhaps leaning towards "tried and true" with the other embracing "new and improved".

To better understand these options for protecting your business operations, let's set out what each is and dive a bit into comparing them.

Backup

The intent of backups revolves around the legacy concept of creating copies of data, applications, and systems for the purpose of restoring them at a later date. Backups can exist as copies of files, virtual machine snapshots, entire VMs, and even application-aware datasets.

Backup copies are typically created on a regular schedule (e.g., hourly, daily, weekly) and are usually stored for a predetermined schedule (e.g., daily backups are retained for a month and monthly backups are retained for a year). Because the focus is on maintaining a backup copy, backups tend to follow the "3-2-1 Backup Rule" which states having "3" copies or versions of your data (including the one in production), "2" different mediums, with "1" copy stored offsite.

One of the latest iterations of this legacy rule is the "3-2-1-1-0 Rule", where the "3-2-1" remains the same, but there should be 1 immutable copy (specifically for ransomware attacks), and 0 backup errors.

Modern Backup software solutions all support the use of cloud storage, as well as those providers that offer cloud storage tiers to help improve retention and lower overall storage costs.

Recent years have seen the evolution of Backup as a Service (sometimes seen as either *BUaaS* or *BaaS*) entering the marketplace, with cloud service providers offering to manage the creation and storage of backups – often as a gateway to recovery services should a disruptive event occur.

DRaaS

While Backup meets the desire to maintain a copy of a given dataset, Disaster Recovery is intent on creating backups of your operations with the specific purpose of recovering that dataset in a matter of minutes if/when a disaster strikes. So, rather than just having a copy of some or all of your environment, the thinking revolves around "how do I plan and implement my data protection in a way that if and when I need to recover, it can be accomplished in the least amount of time?"

To facilitate very fast recovery, disaster recovery (DR) tends to avoid legacy backup methods such as file-level backups and instead uses either the VM snapshot backups or – even better – VM replication to a secondary location to facilitate a nearly real-time copy of production. The implementation of these methods is usually measured in terms of minutes or even seconds to ensure the latest "backup" is as close to production as is possible.

The secondary location can be a second data center in another region or the cloud. Replicated VMs and/or VM snapshot backups are held at the secondary location awaiting a disruption event requiring a failover event – where operations become live at the secondary location in a matter of minutes.

What About the "aaS"?

Oh yes… right. Disaster Recovery-as-a-Service (DRaaS) comes into play when your organization either doesn't have access to a secondary location or doesn't want to pay for one. Instead of taking on the massive capex cost involved in setting up your own second datacenter location, DRaaS allows organizations to leverage a cloud service provider's datacenter as the secondary location, enabling you to execute the same Disaster Recovery effort with the cloud as your secondary location.

Additionally, there is the "service" component, found in the form of the cloud service provider including assistance in the creating, implementing, testing, and executing your DR plans.

I want to reemphasize that the main difference I see between Backup and DRaaS is in their approach to data protection: Backup starts with a focus on making copies of datasets without regard to the impending disruption, while DRaaS starts with the impending disruption, determines what recovery needs to look like, and works backwards to the data protection methods necessary to be resilient should that event occur.

To put it another way, Backups are about *data recovery*, while DRaaS is about *operational resilience.*

Matching up Backup and DRaaS Side-by-Side

Let me use the following comparison table to both recap some of the things I've already mentioned, as well as add in some additional factors that may sway you one way or the other.

	Backup	DRaaS
Cost Model	Capex	Opex
Data Protection Focus	Data, Applications, and Systems	Critical Workloads
Backups		
Method	File, VM Snapshots	VM replication, Snapshots
Managed By	Internal IT	DRaaS CSP
Recovery		
Granularity	List of data sets, applications, and systems to be restored	Scenario-specific detailed plans to recover entire environment
Testing	VM/App validation	Partial or complete recovery simulations
Focus	Restore unavailable data/systems	Recovery of operational availability
Timeframe	Hours to Days	Seconds to Minutes
Target	Primary or Secondary Data Center	Secondary Cloud Infrastructure
Difficulty	Simple restore of affected data, applications, and systems	Complex mix of data, applications, systems, and services to be recovered in a specific order
Process	Manual Restore	Orchestrated Failover and Fallbacks
Managed By	Internal IT	DRaaS CSP

The table above feels a bit academic in nature, so let's dive into what makes the two different when considering an actual disruption scenario for your business to set your expectation for each and to demonstrate the differences in practical terms.

What to Expect from Backup or DRaaS

There are a number of functional differences when your back is against the wall in a disruption scenario and you're now resting on the data protection strategy you've long had in place. To set your expectation of what each methodology will deliver in your time of need, let's take the following example:

> *Your organization has suffered a ransomware attack that has hit the entirety of your servers within your data center. All of your Active Directory domain controllers and most of your application servers are all encrypted. The ransom (as expected) is an astronomical amount, so the executive team is calling on IT to recover operations rather than pay the ransom.*

I'm going to use the following perspectives to talk about how you both prepare and respond to the scenario above using Backup and DRaaS: the *process* used, the *people* involved, the *technology* utilized, and the *recovery result*.

Process

The process from backup of a given resource to when it's recovered due to a disruption event is vastly different when comparing backups and DRaaS. And, as you'll see, one is far better prepared than the other.

Backup

With Backups, the critical systems and datasets are identified, backup jobs selection and frequency established, there's monitoring in place to ensure job success, and potentially even job validation (in the case of backing up VMs). When our Ransomware attack hits, if just a few

systems had been encrypted, a simple restoring of the appropriate backups could have done the job. But since the attack scenario leaves nearly all of your data center encrypted and requiring recovery, there will likely be complications. Let's start with the fact that since you're restoring to an encrypted system, you may need to wipe and partially rebuild that system before restore (depending on what backup solution is in place and how backups were created). There will also be complications around integrations, dependencies, version compatibility, and more once everything is restored. This will require additional one-off troubleshooting each issue post-restore, adding to the true recovery time.

DRaaS

With DRaaS, the recovery for the ransomware scenario above started months before the attack ever occurred. A backup strategy was devised around how to recover from this and other disaster scenarios, using a business impact analysis and risk assessment to establish business requirements, and by aligning requirements around workload criticality, availability, and recovery time and point objectives. For non-critical datasets (e.g., the shared Marketing folder on a file server), a daily backup suffices, but for critical workloads, real-time replication of changes to a secondary site is generally used.

Next, a recovery plan is drafted that takes into consideration application and system dependencies (e.g., Active Directory domain controllers on DNS) so that should a complete loss occur, systems can be recovered in an order that quickly establishes operations with minimal downtime. Depending on the service provider's capabilities, this is often automated using recovery orchestration software to ensure a consistent result.

Lastly, any recovery procedures are tested using live simulations in a secondary environment, testing out the orchestration, and ensuring the environment runs error free. Should an issue arise, changes to the plan and/or documentation of how to address the one-off issue are added.

Testing is critical to the success of your planning! That's why we see in Forrester's *State of Disaster Recovery Preparedness 2023* Report, only as little as 4% of organizations aren't performing some kind of testing of their plan.

The recovery process includes recovering any systems that were already replicated to the recovery environment and an official failover where the environment is reconfigured to use the secondary environment. It should also be noted there is a failback event sometime in the future where the same recovery process is executed in reverse to place production back in the primary data center.

People

The folks responsible for protecting your environment need to have a deep understanding of what applications, services, systems, and data is in place. Ideally, they should have some degree of expertise in recovering those very same resources, as responding to a disruption event – regardless of the approach you use – may not go exactly as planned.

Backup

With Backup, the work will fall to your internal staff who have a fair amount of institutional knowledge around what's in place in your data center and how to support it. They probably have less experience in recovery, as these kinds of events don't happen every day. So, while they should be well-versed in restores, considerations like the restore order, compatibility, and dependencies will probably be figured out on the fly, rather than proactively mapped out.

DRaaS

With *DRaaS*, your organization partners with a service provider that specializes in recovery and works in tandem with your internal team. This means you have an external part of the recovery team being seasoned recovery experts working with the internal part of the recovery team that knows everything about your environment.

Because the DRaaS process includes architecting and testing a data protection approach to specifically recover from a disaster like a ransomware attack, your DRaaS partner can take the lead in executing the recovery plan, ensuring the secondary site is ready to be restored to, launching the orchestration, and starting the recovery, with the internal team standing by. Or, in some cases, it's exactly the opposite, depending on your staff count, internal expertise, desire/requirements over who's in control, etc.

Technology

The tech used in each approach is vastly different from one another and really determines both your backup and recovery limitations, as well as what kind of outcome you will have when the Ransomware scenario hits.

Backup

In most cases, the tech involved is pretty simple:

- Your backup solution
- Local and/or cloud storage
- The Data Center (which supports a virtual environment with which to restore to)

If this is your situation, you are limited most by the data center; assuming you have no replication of hyperconverged architecture in place, you must recover to the same hardware (albeit with virtual resources) that production runs on. It also limits the kinds of backups (again, assuming there's no replication here – just backup copies of production data, applications, and systems).

The result in our ransomware scenario is it's likely going to take longer to recover than just the restore time, adding to the remediation duration and cost.

DRaaS

Unlike Backup, DRaaS involves the addition of a cloud-based secondary site *which changes everything*. With a secondary site, there are a few added options that improve your recovery:

1. You can choose a hot or cold secondary site – Some orgs choose to spin up a recovery site when needed while others choose to have it running all the time. Some go a hybrid route where only critical workloads are running all the time with everything else being spun up at time of recovery.

2. You can test recovery of *everything* – You now have the option to test out the recovery plan in a live simulation that can include everything from a single server to the entire environment.

3. You can leverage replication – replication requires there to be somewhere you replicate *to*. With a secondary site, you can keep some or all of the environment running-in-wait until a recovery is necessary – at which time, it's just a matter of a failover (which takes minutes) rather than restoring system after system after system to get the same result.

The end result of having the secondary site is recovery takes far less time. Just having the site available as a cold site would improve the speed of the process of recovering operations. Add in the ongoing replication of critical workloads and recovery of that part of operations becomes almost instant. And, for everything else, the ability to test recovery plans and orchestration – and be able to modify the plan to address issues before an actual disruption event – improves the predictability of your recovery while reducing the overall time of recovery down to seconds or minutes, rather than hours or days.

Face it, Backup is NOT DRaaS

I'm hoping by now you can see that these two data protection methods are most definitely *not* the same. And that's important; when you begin to see the need to keep the business running, you can use an approach that starts with the technology (Backups) and works toward the business need. You need to use an approach that comprehensively starts with the business need and works toward the tech that will help you achieve those recovery goals.

So, if you're going to stay on Backup for the time being or switch to DRaaS, allow me to at least spell out a high-level process for developing a proper data protection strategy (that you will fit in your approach as best it can):

1. Perform a Business Impact Analysis – this involves identifying the potential impact on your business resulting from any kind of loss of operations. This analysis should provide you with an idea of which functions are important to the business.

2. Do a Risk Assessment – this helps you measure the risk a given disruption scenario (e.g., ransomware attack, loss of a location, downed critical application, etc.) would have on the parts of your operations identified in the Business Impact Analysis. The identified risks should then be prioritized based on the likelihood and potential impact, providing you with a matrix of operations and risks where you need to place your priority.

3. Determine the Gaps – Examine what it's going to take to properly protect the identified workloads, applications, and data should one of the prioritized risks come to fruition. Then look at what your data protection technology, processes, and people can do today. The difference between the two are your data protection gaps that *must* be addressed.

4. Build a Recovery Plan – even if you are sticking with Backups, you'll need a plan of how you'll perform the recovery itself that addresses recovery order, dependencies, compatibility, use of a secondary site/data center, etc.

5. Test the Plan – If you can't do any full or partial simulations, at the very least do a tabletop walkthrough every six months to ensure that those involved are familiar with the process, should it need to be used.

If you've come to the conclusion that you should be using DRaaS, much of this comes with engaging with a DRaaS service provider who will guide you through every step to ensure you can achieve proper recovery or resilience.

The Big Takeaways

I think we all agree on the necessity to protect the business, its operations, and the underlying technology bits that make that up (servers, applications, services, data, etc.). The question then becomes *how do you best provide protection in a way that doesn't just put each of the tech pieces back into operation, but does so in a way that doesn't add to an already negatively impactful disruptive event?*

Backup and DRaaS are vastly different approaches to how that protection is achieved. In fact, the very degree of what can be achieved is up for discussion when comparing the two.

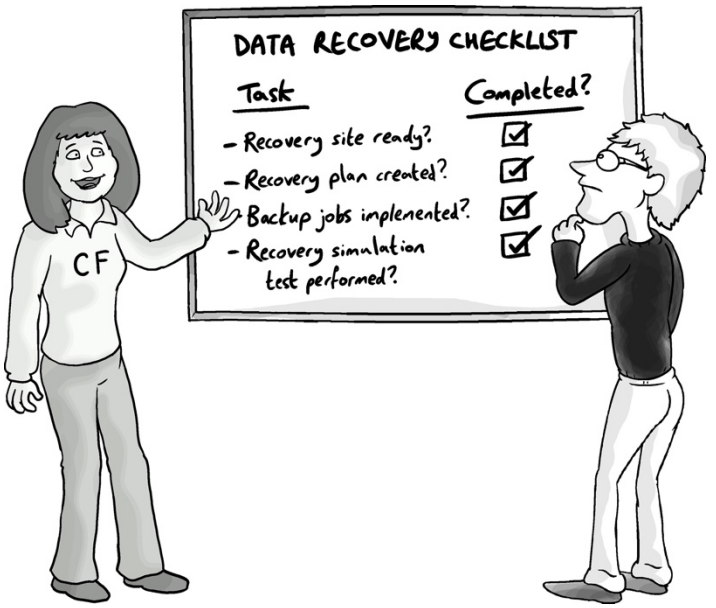
Backup remains a viable choice for those organizations that aren't as concerned about recovery until they need to be. But if you've read this far, I suspect you realize the importance of starting with the end recovery result and working backwards to identify those technologies, processes, and people that are going to get you there.

DRaaS takes Backups and adds to it business context, operational focus, proactive planning, augmented staff, expert assistance, faster execution, and a more predictable result – all at a reasonable cost.

I've spent the last 20 minutes or so of your time educating you on why the two aren't the same and placed some emphasis on why you should be thinking about DRaaS. At the end of the day, I want your organization to be better protected and more able to be resilient in the face of even the worst disruptive event.

Just be sure your approach is going to get you there.

Sponsor Chapter – CyberFortress



Today's business leaders assume that in the event of an outage, the organization is able to recover much more quickly than is actually possible. Most IT organizations are thinking of doing some form of disaster recovery, or – at very least – taking an approach that leverages the cloud to try to alleviate this.

When compared to traditional backup, it's easy to think of using the cloud and implementing a true DR strategy as a complicated and expensive venture. If you were to go about it on your own with little-to-no experience in DR, that's a fair assessment; your journey will likely be riddled with wrong decisions, potentially costly mistakes, inadequate planning, poor execution, and unpredictable results.

That's one of the reasons this eBook isn't comparing Backups to just DR; it's about making the jump with both feet into leveraging a service that doesn't just "do the work" for you, but ensures you have a recovery plan that will work.

CyberFortress

CyberFortress is a global company that makes it simple to fully backup and rapidly recover all lost or stolen data. They provide highly available and secure cloud data protection Disaster Recovery (DRaaS) and Cloud Backup (BaaS) solutions, built on world leading technology from Veeam. By partnering with Veeam, CyberFortress has supported literally hundreds of thousands of physical and virtual machines globally, preventing damage and disruption to organizations of all sizes throughout its' 20+ years of providing world-class data protection and recovery solutions.

DRaaS is CyberFortress's core competency, employing a team of Credentialed Recovery Specialists with years of experience who are all Veeam-certified as architects or support engineers to tackle the even the most complex disaster recovery needs.

A number of factors differentiate CyberFortress from their competition:

Data Centers

Their global data center footprint spans across North America, Europe, Australia, and New Zealand, leveraging Tier 4 and 5 facilities to provide the highest levels of security, redundancy, performance, and availability. Meeting the needs of a diverse set of customers, CyberFortress's data centers adhere to compliance regulations, including SOC 2, ISO 27001, PCI-DSS, and HIPAA.

Hardware

In most cases, the hardware used by CyberFortress either matches or exceeds the quality of that used in the production environments of their customers. For Premium BU services as well as DR services, data

resides on Cisco Nimble storage to provide best-in-class performance in a failover state, with HPe-branded server hardware used as the foundation for their hypervisor-agnostic recovery environments that can run on hypervisors from VMware and Microsoft (with customer software requirements meeting the compatibility matrix for the selected hypervisor).

Expert Help

Organizations without internal staff that have performed disaster recoveries many times before need to rely on a partner that has… a hundred times over. CyberFortress acts as an extension of your internal team, bringing the necessary expertise to the table to architect, plan, design, implement, orchestrate, test, optimize, and execute a disaster recovery effort – but does so using a measured approach based on the customer's needs. From simply providing as-needed assistance to completely turnkey "white glove" service, CyberFortress provides tailored services to ensure you have the specific help you need to make recovery successful.

Service Delivery

CyberFortress' services are comprehensive, ensuring both technical and business needs are met. It starts with being hypervisor-agnostic, allowing them to assist your organization with its disaster recovery needs regardless of virtual platform used. Virtual workloads begin their replication using an included seed drive service, allowing the fast implementation of a secondary recovery site.

Once a recovery environment is architected and a recovery plan is created, CyberFortress walks customers through failover and failback testing, looking for gaps in the process and documenting results to update the recovery process. Customers are given a disaster recovery drill report to show leadership the last test performed, along with how long it took to complete, what issues were experienced, and more.

Affordability

DRaaS doesn't need to be expensive and can actually be delivered as a cost-effective disaster recovery option. By offering DR as a service, CyberFortress can eliminate hardware and software costs, reducing your financial burden down to a monthly operating expense that fits your budget.

In addition, by getting your recovery point and time objectives down to minutes, the net cost of recovering from a disaster and returning to normal operations is a fraction of that of Backups.

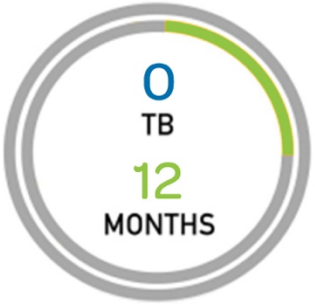
Protecting your Business with CyberFortress

Organizations like yours face the challenge of putting together an operational resilience and data protection strategy using what technology and budget they currently have. But as the organization evolves, those needs also grow, making it difficult for IT to scale their current strategy to meet the need.

CyberFortress makes transitioning from internal Backups only to a full DRaaS-based resilience strategy easy, fast, effective, and affordable.

CyberFortress™
The Recovery People

CLOUD BACKUP VS DRaaS



Storage Size

0 15 25 35 50

Contract Length

12 18 24 30 36

MONTHLY ANNUAL

VEEAM
Cloud & Service Provider
Platinum

CALCULATE PRICE

Quickly become conversational about Backup and DRaaS

We can all agree on the necessity to protect the business, its' operations, and its' supporting technology. The question is how we best provide the necessary protection. Backup and DRaaS offer vastly different approaches to how that protection is achieved. In this book, I'll discuss those differences and explain how DRaaS takes Backup to the next level and ensures your organization is better protected and more able to be resilient in the face of even the worst disruptive event.

About Nick Cavalancia

Nick Cavalancia is a 4-time Microsoft Cloud and Datacenter MVP, has over 25 years of enterprise IT experience, is an accomplished consultant, speaker, trainer, writer, and columnist. He has authored, co-authored and contributed to dozens of books on various technologies, and regularly speaks, writes and blogs for some of the most recognized tech companies today.