Confusion as a Service

The problem with “as a Service” and Disaster Recovery today

CyberFortress™
The Recovery People

cyberfortress.com
855-223-9322
sales@cyberfortress.com

Introduction

Having "aaS" Recovery That Aligns With The Disaster

You've, no doubt, experienced some kind of disaster recovery event. I could have been something as big as a complete loss of location and services, or the outage of just a specific application. No matter how big or small, when most of us go through our first disaster, we figure out on the other end that your ability to respond was a bit slower than desired and, quite possibly, the outcome itself didn't go exactly as you thought it would.

We're writing this ebook under the assumption you have something in place - on-premises file or image-based backups, use of the cloud for storage or recovery, a co-location – and maybe even something a bit more elaborate that includes one of the various flavors of "aaS"-type recovery.

Whatever it is, you're likely reading this ebook because your current strategy didn't meet the organization's requirement in its' time of need.

The challenge is to proactively address the recovery specifics for a disaster that hasn't happened. You either attempt to guess all the potential disasters that can occur, the losses from each, and work backwards to the types of recovery services that will assist. Or, you look at the operational needs of the business, determining what the recovery requirements are for each critical workload, and determine how the various "aaS" recovery offerings can assist in meeting your recovery objectives.

This ebook focuses on the challenges created from the many different cloud-based recovery services offered today – and how to identify the right one to meet your organization's needs. Over the following 5 chapters, this ebook will educate you on various cloud-based services available, and provide guidance on how to choose the right one:

Confusion as a Service:

The Challenge of DR and "aaS" Today

Let's assume that you fall into one of two categories. Either you have no cloud-based recovery services employed at the moment and are trying to figure all this "aaS" out, or have some kind of recovery-related "aaS" in place, but you're not sure if it's the right one. In either case, you know you need to get this right – after all, recovering from a disaster is already stressful and doesn't need the added pressure of potentially becoming a "resume-generating event". Take the following actual scenario of a clothing company based in New York City during the aftermath of a real-life disaster –2005's superstorm Katrina.

> After the storm hit, the streets were completely flooded 2 blocks away, the first floor offices were flooded out, and power only existed on select floors (resulting in the company even considering running extension cords outside the building between floors). There was no Internet, and – more importantly – no communications. With all operations, applications, and services – to both their staff and customers – residing in this building, the company was facing a true crisis.

While none of us ever hope to be in a scenario as dire as this, it's an all-too-common scenario: reliance upon on-premises technology to protect the business – even in a disaster where the premises itself becomes unusable.

So, why do companies not embrace cloud-based recovery services?

In this chapter, we'll discuss the reasons why confusion exists around choosing and using cloud-based recovery services, offering some guidance around how to eliminate the confusion.

Finding the Source of Confusion

At the end of the day, you're keenly aware you need some or all of your operations to be functional – no matter what the circumstances. And yet, the proper means to leverage various recovery-related, cloud-based services still escapes you. The reason is two fold:

- Not enough clarity around the services offered
- A disconnect between what you need and what they offer

Defining the Service in "As A Service"

So, which "aaS" do you need – Backup? Recovery? Disaster Recovery? Business Continuity? Platform? Application Platform? Infrastructure?

And, because there are so many vendors vying for your attention to their service as the answer to your problems, unfortunately, the list above actually could continue beyond just those listed. Rather than trying to all agree on one term to use, each vendor wants to differentiate themselves – and, in the process, it only creates more confusion.

To add insult to injury, not every instance of a given service means the same thing – the same service term can mean different things to different service providers. For example, some vendors offer hands-off, "white glove" recovery under the name DRaaS, while other companies delineate DRaaS as more designated infrastructure for you to use when you want to perform any recovery actions, and then reserve the term RaaS to define the full-service recovery option. This mismatch of names to services across vendors isn't entirely at epidemic levels, but it exists enough that you need to be aware of what tangible services are actually being offered.

Are your needs misaligned with what they offer?

Confusion also exists because many IT organizations don't actually know what kind of recovery they need. This is because of an IT-centric approach to disaster recovery – one that looks at the recovery process from more a per data-set, per system, or per-application basis. The problem with this is, while it will certainly define what needs to be recovered in a disaster, it does little to align your recovery needs with these strategic recovery services.

If you're currently approaching recovery in the "per-recovery set" mentality, you're thinking far too tactically; nearly every recovery service is thinking strategically how to get your business back up and running. And the two don't align.

That clothing company was both unprepared – even from an IT-centric recovery approach – and uninformed about what their recovery options were via the cloud. In the end, they physically drove their servers to a cloud service provider and reconfigured them there – an effective, but certainly not optimal way to respond to the disaster.

Focus on Critical Workloads First

Organization with more complex operational environments likely have more confusion than those with simple recovery needs. Complex environments require defining critical workloads separate from the remainder of operations and establishing recovery time-frames for these specific workloads. In your time of need – regardless of the "aaS" you choose to utilize – it's these systems, applications, services, and resources that are going to make the business "operational" as quickly as possible.

Understanding Service Scope

Because of the critical nature of the topic, there can be no misunderstanding as to what's offered and included, and what's not. When speaking with a cloud services provider, ask about the scope of services around backup, recovery, who's responsible, what's the SLA, who performs the work, and what does failover and failback look like.

Getting a complete picture will help you comprehend what each vendor offers, how they differ, and which one can assist.

Eliminating the Confusion

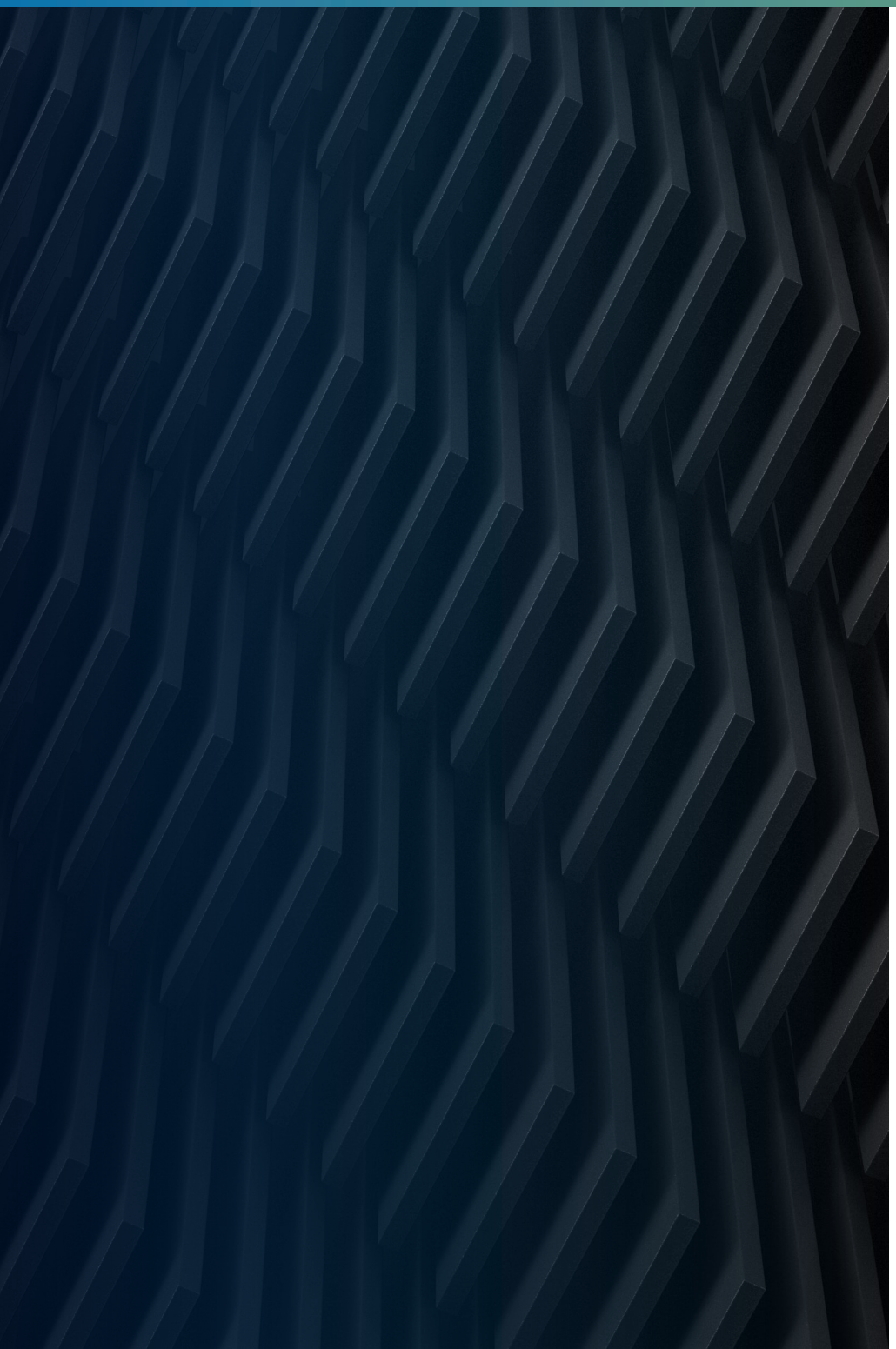
To eliminate the confusion, you obviously need to be informed – both as to what specific recovery services are being offered, and – more importantly – what your really recovery needs are. We'll actually clear up the confusion around recovery services in the next few chapters of this ebook. The tougher part is on you, before you look at any kind of cloud-based recovery service.

You need to first start with business objectives and work backwards to recovery. Think about the simple enough "disaster" scenario of a complete loss of operations, and begin to work through each service, application, system, and data set used within the business - what kind of impact will the organization feel when each goes down or is unavailable? Craft the response in tangible terms to the business – financial, reputation, productivity, etc.

When it comes to each of those operational aspects of the business, what kind of failover does each require? Is it 2-minute? 4-hours? What? This is normally answered by defining a few recovery time-frames:

- **Recovery Time Objective (RTO)** – the targeted amount of time for a given recovery to take.
- **Recovery Point Objective (RPO)** – the targeted amount of data lost once the system or application is recovered.
- **Maximum Tolerable Period of Disruption (MTPoD)** – This is the maximum amount of time the organization can take to recover before the impact is materially greater than just losing a few sales or wasting some employee time.

Once you have these strategic time-frames defined for each of your services, applications, systems, and data sets, you can build out a tiered set of criticalities, which can then be aligned to recovery services by engaging with a partner specializing in cloud-based DR.



Getting to the Right "aaS"

You know what's important to your business; what's necessary is to identify and select the right service or services that will meet your business' recovery objectives in its time of need. By working through the services and applications your organization relies upon, and defining your recovery needs, you place your organization in a position where it becomes obvious as to whether a particular cloud-based recovery service is the right fit or not. It should be noted that, based on your internal requirements, the answer might be a hybrid approach of a number of services. So, don't go into this thinking there's only one right answer; it's far more likely you may have a few approaches to use, that will minimize your investments, while maximizing your needed recovery.

In the next chapter we'll begin a multi-chapter examination of the 3 most effective recovery services available today, starting with Infrastructure as a Service. We'll define what's entailed in this service, what are the DR benefits, when it's the right choice, and what kind of organizations it's best suited for.

Infrastructure as a Service:

Less Reacting, More Readiness

At the core of a disaster event is the need for an environment in which to recover. In some scenarios, just having an on-premises virtual server to recover a single system meets the need. But in enterprise and complex environments, an on-site data recovery from a disaster of material proportions is likely impractical – data center complexities, tiered applications, and system dependencies all create a rather complex set of infrastructure requirements that usually won't just be lying in wait on-premises.

Having infrastructure ready as part of a recovery plan is a valuable foundation (pun intended); it establishes where recovery will take place, and acts as the basis for all subsequent recovery planning. In essence, it takes some of the "unknown" of DR away, giving light to how the environment should look when the dust settles.

But what exactly is Infrastructure as a Service (IaaS)? Or more importantly, what can you assume it will do for you in your time of need?

Defining IaaS

As mentioned in chapter 1, there can be a lot of confusion around what is included/offered with IaaS. In plain and simple terms, IaaS is defined as on-demand online computing resources including CPU,RAM, and disk space. While there are other bells and whistles IaaS providers will tout, at its core, IaaS is you renting hardware that sits in the cloud.

IaaS is, in many ways, a lot like renting a high-end supercar for a day – you get to use the most powerful and reliable hardware possible, only using it when you want it, and only paying for it when you use it.

IaaS as part of your DR Strategy

Because IaaS is simply on-demand hardware and not a DR-specific offering, you might think it's only used during an actual DR event. Hardware is spun up, images are moved or recovered, and the cloud infrastructure becomes the primary site. In reality, this scenario requires a much more detailed use of the cloud infrastructure well before the DR event. Hardware needs to be spec'd out, testing of the cloud infrastructure needs to be accomplished, and a method of getting backups into close proximity of the cloud infrastructure needs to be established.

Today, cloud infrastructure's normal use is a bit of a hybrid between DR and infrastructure, where organizations are less thinking about using it to react to a DR event, and, instead, be ready for one should it happen. For example, critical workloads that need to be "always on" (e.g. email, website, ecommerce) utilize secondary servers running in a cloud infrastructure to keep those workloads continually running. In other cases, some applications, such as an ERP system, don't have great way to backup and must use that vendor's solution – in this case, it makes more sense to have the application run in the cloud for higher availability.

The best use of IaaS is one where it is utilized to keep the business operational every day – including when a disaster occurs – and not to simply be considered as a duplicative network environment where recovery takes place should it be needed. The result of the BIA is a set of interview answers that should provide you with an idea of which business functions are, in general, important to the business. It would be helpful to use the results of the BIA to establish a fundamental prioritization of functions based on the responses. This will help the Risk Assessment be more impactful, as it can be focused on those business functions that the organization obviously cannot do without.

Not all IaaS is the Same

In practical application, not all infrastructure offerings are equal. Sure, there's compute and storage, but the data centers which service these offerings vastly differ from one provider to another. CyberFortress uses Tier IV Gold data centers that are designed to provide maximum operational sustainability.

With redundancy, security, and availability as a top priority, these data centers serve as the critical foundation for CyberFortress' recovery services leveraging the Veeam Availability Suite.

Who is IaaS best suited for?

There are a few organizational needs that help best define whether IaaS is best suited for your organization. In general, IaaS is a fit for those organizations needing:

- **Manageability** – Organizations that want complete control from A to Z should look at IaaS. Many cloud environments simply provide service level agreements around performance and availability. Cloud infrastructure is managed by internal IT, so every aspect of the environment – from IOPs, to RAM, to bandwidth, to CPU – is visible to you and under your control.

- **Extensibility** – Organizations needing to expand their data center footprint utilize IaaS as a means to both offset operational risk, while simultaneously extend their environment without taking on massive capital expenditure.

- **Flexibility** – Organizations that want to dynamically use additional infrastructure leverage IaaS, expanding and contracting their usage to meet the current needs of the business.

- **Operational Performance** – Organizations that desire to operate within the same size and caliber of dedicated data center their larger enterprise counterparts enjoy – but without the huge price tag – are perfect for IaaS. Those managing TBs of data daily are a perfect fit. Some organizations look to consolidate existing data centers, while others simply need higher degrees of security, performance, and availability than they can provide on their own.

- **Proactive DR** – Typically DR efforts begin once the disaster hits. IaaS is perfect for those organizations that would rather proactively establish and utilize cloud infrastructure for both daily operations, being already prepared should a disaster impact the on-premises network.

Benefits of IaaS

While the list above can somewhat be interpreted as a benefits list, it's important to clarify these are a generic list and may or may not be available with every IaaS vendor.

- **Dynamic** – Unlike your on-premises hardware, IaaS environments can adjust resource pools and leverage burstable bandwidth to increase performance, meeting any workload requirements. From the smallest of servers needing a single virtual CPU and a few GBs of RAM, all the way up to critical workloads requiring as much as 1PB of RAM and 1000 virtual CPUs, IaaS is designed to deliver the needed performance.

- **Secure** – IaaS providers take security seriously, utilizing multiple layers of physical and network security to ensure your systems, applications, and data are safe. Any IaaS vendor worth their weight meet compliance initiatives such as SAS-70, SSAE-16, PCI, HIPAA, and ITAR to demonstrate their strict adherence to process, policy, and controls that ensure the highest levels of security.

- **Reliable** – The intent of every IaaS provider is to keep you operational. So, every part of the infrastructure has redundancy; networking, storage, compute, firewalls and more – all in an effort to maximize your uptime.

What about Cost?

From the DRaaS provider's perspective there are countless variables when you consider all the potential customers' environments and how different they are from one another. Add to that the fact that the overarching promise of a DRaaS provider is "we'll get it back up and running." So, pricing tends to be rather simplified down to just a cost per TB of data. Some DRaaS providers pre-package failover time into the cost – for example, 30-days of runtime with specific sets of resources. Other providers go more a bare bones route with a minimal cost per TB, charging for incurred compute (CPU and RAM) when recovery occurs.

Eliminating the Confusion: DRaaS

DRaaS is about partnering with a provider to define a plan and an environment that facilitates fast recovery of your organization's most critical workloads. While truly defined by the gaps in your organization's expertise or execution ability, the use of DRaaS with a trusted provider does instill within the organization the confidence that, should a disaster event occur, operations will continue within minutes.

In the next chapter, we'll take a look at Backup as a Service (BaaS) in the same manner as this chapter, outlining what it is, who is it best suited for, and when is it the right option for your DR needs.

IaaS Offerings Should be Tailored

Organizations should be thinking about their specific needs and looking for partners that tailor the IaaS-based solution. For example, orgs may want more/less hands on, or want DR included.

CyberFortress offers uniquely-designed IaaS solutions catering to the operational requirements of each of their customers. Additional needs around backup and disaster recovery using cloud-based infrastructure are met through CyberFortress' partnership with Veeam to facilitate intelligent orchestrated and automated recovery.

Disaster Recovery as a Service:

Up and Running as Fast as Possible

To remain competitive today, many organizations feel the pressure – and, therefore, strive – to be down as little as is possible. We used to count this in percentages – like the "five 9's of availability", but in recent years, this has (thankfully) changed to the far more practical and tangible use of an amount of time. Today, this need to have services and applications available to customers and employees alike is so great that downtime itself is now measured in counts of single-digit minutes.

Traditionally, recovery is a function of backup – only maintain a daily backup, and there's no way you can possibly recover to within minutes of a disaster. No, recovery of this caliber needs a different kind of DR strategy– one where data is replicated, rather than backed up; where standby services and applications are lying in wait, rather than require a lengthy data restore to be operational; and where recovery is more about a single simple network failover than about a complex recovery of multiple systems and applications. A recovery like this is what empowers businesses to recover in mere minutes.

While you may think "That's it! That's the one for us!", DRaaS isn't for every organization, or even every application.

So, what is Disaster Recovery as a Service (DRaaS) and when is it the right choice?

Defining DRaaS

DRaaS should be thought of as means of achieving simplicity in your failover and failback during a disaster event. This is accomplished through the right mix of your internal IT and the provider. Depending on the provider and your organization's specific needs, some organizations only need the provider to help build and/or test the DR environment. Others look to leverage the provider for complex legacy solutions that involve a lot of detail around the recovery. And still other organizations are looking for some level of assistance – up to and including "white glove" service – around the failover, the failback, or both.

The beauty of DRaaS is that it is defined as leveraging a provider, as needed, to ensure recovery is simple, effective, and efficient.

DRaaS as part of your DR Strategy

In a typical DRaaS scenario, everything needed for a recovery should already in place - on boarding of data and applications is complete, internal and provider teams are sync'd up on failover processes, servers and services are replicated, and the recovery environment is configured for failover. The only thing left to be done is the failover itself during a disaster event.

So, to make this happen, your DR strategy is more about helping the DRaaS provider define the scope of the recovery, including which systems and applications are to be included and the expected recovery objective time-frames (previously discussed in chapter 1):

- **Recovery Time Objective (RTO)** – Your DRaaS provider will be asking you how long will you allow the recovery to take? Or, put differently, how much time are you willing to be down?

- **Recovery Point Objective (RPO)** – Your DRaaS provider will need to understand how much data are you willing to lose (which determines the recovery point in time).

Both of these objectives need to be defined on a per workload basis, as some critical systems may be fine with a 15- or even 30-minute RTO and RPO. But more critical workloads may require these objectives to be more like seconds from the initial keystroke that starts the recovery.

To ensure a successful DR strategy, defining what parts of the recovery process – from defining backups, to building the recovery environment, to establishing, testing and executing recovery plans – need to be handled by the DR provider. Once this is defined, you now have an understanding of where DRaaS – and the chosen provider – will help to achieve your recovery goals.

Sometimes Recovery Isn't Fast Enough

Some workloads have very specific and extremely low recovery objectives. So much so that any kind of recovery process – even one that takes single-digit minutes – isn't practical.

In cases like this, CyberFortress leverages Veeam Backup & Replication to continually replicate critical workloads up to their world-class cloud-based infrastructure, proactively addressing DR efforts with a copy of your critical workload lying in-wait.

Who is DRaaS best suited for?

While DRaaS sounds like it's the perfect answer to every organization's DR woes, in reality, it isn't for everyone. Typical organizations that employ DRaaS have the following characteristics:

- **Have Critical Workloads** – No DRaaS provider is going to tell you that can't put anything less than a critical workload into their data center, but given the investment that is put into planning a recovery, DRaaS aligns better with those workloads that will have a material impact to the organization's bottom line if they aren't up and running quickly. (However, it should be noted that some organizations do choose to have their entire environment recovered via DRaaS.)

- **Are Looking to Recover** – it may sound redundant, but it's an important nuance. Unlike IaaS customers (who proactively put redundant services into a cloud infrastructure in preparation for a disaster), DRaaS customers are wanting a service that allows them to keep operations running within the company's data center(s), and leverage cloud-based resources during a disaster event.

- **Are in Regulated Industries** – While you certainly don't need to be, many DRaaS customers are in industries such as legal, healthcare, or finance. They utilize DRaaS because it both meets their DR needs, and because the security and processes providers generally use to adhere to compliance mandates are more strictly and strongly implemented.

- **Don't Mind Being a Bit Hands Off** – As previously mentioned, you're trusting some parts of the planning and execution of a recovery plan to a provider, so organizations leveraging DRaaS tend to trust the provider's expertise both before and during a disaster.

- **Aren't Control Freaks** – Because the recovery environment and everything in it is managed by the DRaaS provider, organizations typically have little control over and visibility into the infrastructure on which their recovery environment sits.

For those workloads that simply can't be down, DRaaS represents the ultimate in understanding every detail about the needed recovery process, leaving no technical stone unturned – all in an effort to guarantee delivery of a working system within minutes or seconds. Some of the benefits of DRaaS include:

- **Planned** – In practice, DRaaS is probably more planning than it is even recovery. DRaaS providers sit with your IT, security, and applications teams to understand the specifics around resource requirements, application dependencies, and recovery objectives.

- **Tested** – Most DR plans aren't worth the paper they're printed on, because they're never tested. Because the recovery process of critical workloads is a complex set of steps that need to be one in order – and without error – to be successful, DRaaS generally includes quarterly or semi-annual testing of the recovery environment and process. This is done to ensure recovery objectives can be met, the recovery process works, and to identify and address any issues during testing that could come up during a real disaster.

- **Timely** – Recovery scenarios where internal IT does the work themselves using whatever means are available at the time of the disaster event only results in a lengthy recovery process that produces less than desirable results. DRaaS planning and testing are done to build a solution that ensures RTOs are met for each workload, resulting in service availability that meets your expectations.

What about Cost?

IaaS can provide the same dynamic performance, security, and reliability you'd experience by putting your own hardware in a SuperNAP, but at a lower cost. But there are a number of common ways IaaS is priced, so your mileage may vary here.

The first is based on providing and charging for dedicated hardware. This has obvious implications around utilization, but some critical workloads perform better on physical hardware over virtual environments. Another common option is to offer pricing based on resource pools (for example, every 2 CPUs and 2 GBs of RAM). You will find this pricing to be flat with some IaaS vendors (so the smallest and largest customer get the same price), and tiered with others. To ensure IaaS is cost-effective for your organization, it's important to understand your specific potential usage of IaaS, the pricing model of the provider, and resultant cost therein.

Eliminating the Confusion: IaaS

IaaS provides organizations with the opportunity to leverage enterprise-caliber data centers without the need for a material investment in hardware, time, and personnel. From a DR standpoint, IaaS provides organizations with the ability to proactively establish their recovery stance, but by putting critical workloads in place now – rather than after a disaster – and use those implementations as part of operations. In the next chapter, we'll take a look at Disaster Recovery as a Service (DRaaS), following a similar path as in this chapter to outline what it is, who is it best suited for, and when is it the right option.

Consistent Recovery

Testing helps make certain the recovery process will work, but workload dependencies can create specific execution requirements at the time of actual recovery. The key is to consistently execute the plan – both at testing time and in a recovery scenario.

CyberFortress automates the process of creating, documenting and testing disaster recovery using Veeam Availability Orchestrator. This ensures the same process used during successful testing is the same one used in the middle of a disaster.

Backup as a Service:

Data Protection in the Cloud

The success or failure of a recovery rests solely on whether you have the right backups in place. No backups, no recovery. Sometimes all that's needed is a solid plan around what should be backed up, based on the likelihood of any given disaster event. With this in hand, organizations can craft a backup strategy that will provide appropriate data protection at the time of recovery – whether the "disaster" is the simple loss of data, the loss of an entire data center, or anything in between.

While a riskier position, some organizations choose to focus their efforts on ensuring recoverability through proper backups into the cloud, relying on a partner to assist with the recovery specifics when the time comes. This methodology keeps internal IT in the driver's seat, with full visibility into what data is protected, and how the backups can be utilized when necessary.

So, what's entailed in Backup as a Service (BaaS) and what role does it play in a DR strategy?

Defining BaaS

BaaS is less ambiguous than the other services mentioned in this ebook. In a tactical sense, it comes down to two things: cloud-based storage to host backups and management of backups. BaaS provides the organization with access to all the space needed – along with the bandwidth, compute, etc. all necessary to support the storing and retrieving of backup data. Generally, BaaS is an unmanaged offering, with the simple obligation on the part of the provider to keep the backup data target up and running.

In most cases, management of backups is also offered – going beyond just "we store your data". This includes the monitoring of backup jobs, proactively reaching out to the organization when jobs fail, and potentially the service of fixing any issues related to an unsuccessful backup. A true partner tends to want to do the management for the customer to not just facilitate backups storage, the goal is to provide end-to-end services around backups to ensure your data is protected.

BaaS as part of your DR Strategy

While backup seemingly has little to do with the actual recovery process, in reality, it's a critical step. So, choosing what, how, and where you backup will determine the level of recoverability possible. The use of BaaS takes this a step further, as the use of the cloud backup provider that can help with your recovery efforts makes getting recovery assistance in your time of need as easy as placing a phone call.

The right BaaS provider should already be thinking along those lines, offering to ensure that you are not only backing up critical workloads, but are doing so in a way that maximizes your recoverability and minimizes the time to do it.

So, even as you may only be considering BaaS (as some organizations are not ready to dip their proverbial foot into the DRaaS pool), keep in mind that backups should be created with as easy a recovery as possible in mind.

Sometimes Recovery Isn't Fast Enough

In a world where very fast (and accurate) recovery seems to be all everyone is talking about, it's reasonable to wonder when should you choose BaaS. The answer lies in your organization's needs. For example, you may only require assistance designing and executing a cloud-based backup strategy, but have internal expertise to perform the recovery. Or when you have very specific backup requirements around massive amounts of data and need a partner to cost-effectively define a cloud-based backup strategy and provide the storage. In scenario's like these, leveraging a BaaS partner is likely the more appropriate answer.

CyberFortress provides BaaS in conjunction with Veeam Backup & Replication to create a tailored backup strategy that facilitates the protection of your organization's data. And should you require assistance with recovery, the same partnership can be leveraged to help if external help is required.

Who is BaaS best suited for?

There are a few types of organizations that are interested in BaaS.

- **Those needing more than on-prem** – This applies to just about any organization on the planet; on-prem backups mean recovery itself becomes a disaster if the physical location is wiped out. Having cloud-based backups gives organizations the ability for anytime, anywhere, any loss recovery.
- **Organizations with little or no IT staff** – Managing backups themselves is nearly impossible and passing the work onto a trusted partner makes both financial and technical sense.
- **Larger organizations with lots of data** – Those with tens or hundreds of TBs of data look to BaaS when they are only concerned about having the data accessible, and choose to worry about DR at a later time.
- **International organizations** – BaaS providers tend to have data centers globally, allowing for backup data to be securely stored without the fear of extradition by foreign governments.
- **Organizations testing the "aaS" waters** – In both cases, BaaS can serve as the entry point to test out the provider and then add on services later.

Benefits of BaaS

For organizations that fit the demographic of a typical BaaS customer, this service offers organizations with the absolute assurance that their data will be available should a disaster strike, while leaving the recovery details to internal IT. But the benefits of BaaS don't stop there; other benefits include:

- **Lower TCO**– the cost of maintaining your own data center (or even just leveraging a private cloud and managing the backups yourself) is more costly than utilizing an end-to-end backup service.
- **Simplicity** – This service requires little effort on the part of the organization. Backups are defined with the provider, jobs are monitored, with the customer being notified when there's a problem.
- **On-Prem Performance** – Cloud backup today is anything but slow. With technologies like incremental block level backup sets, deduplication of data, and bandwidth throttling, the actual amount of data being sent up to the cloud is minimal, while still maintaining a complete backup of your environment.
- **More Options than On-Prem** – With data residing in the cloud, organizations can choose to restore to cloud-based virtual environments, an alternate location, etc., providing more recovery options that on-premises tape or disk backups offer.
- **Access to Additional Recovery Services** – BaaS providers are wanting to offer you the right services that meet your recovery objectives, methodologies, and budget. By having your backups stored with a provider that offers DRaaS, making the next step up to ensure recovery is much simpler than for those starting out looking for a DRaaS provider.

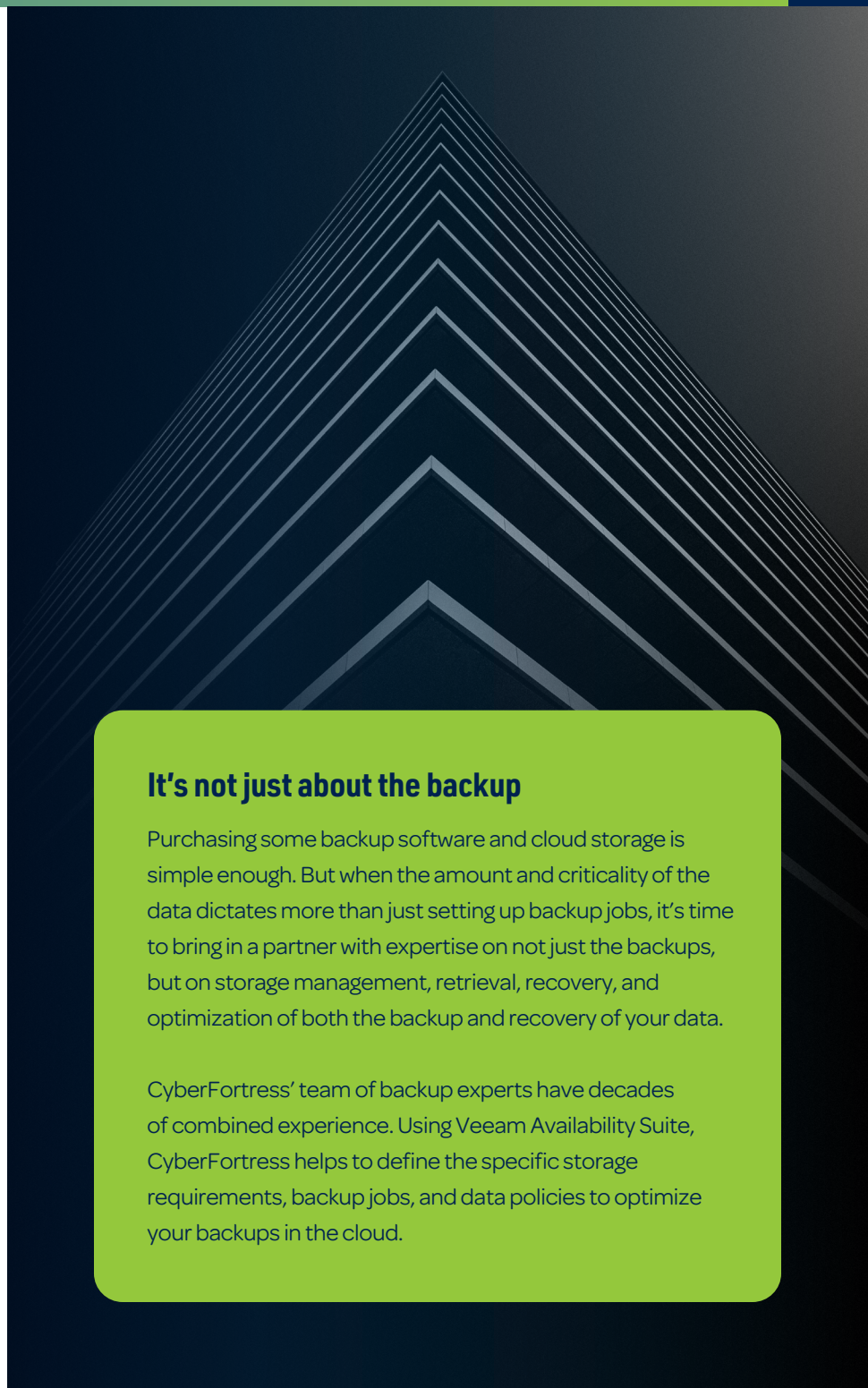
What about Cost?

From the DRaaS provider's perspective there are countless variables when you consider all the potential customers' environments and how different they are from one another. Add to that the fact that the overarching promise of a DRaaS provider is "we'll get it back up and running." So, pricing tends to be rather simplified down to just a cost per TB of data. Some DRaaS providers pre-package failover time into the cost – for example, 30-days of runtime with specific sets of resources. Other providers go more a bare bones route with a minimal cost per TB, charging for incurred compute (CPU and RAM) when recovery occurs.

Eliminating the Confusion: DRaaS

DRaaS is about partnering with a provider to define a plan and an environment that facilitates fast recovery of your organization's most critical workloads. While truly defined by the gaps in your organization's expertise or execution ability, the use of DRaaS with a trusted provider does instill within the organization the confidence that, should a disaster event occur, operations will continue within minutes.

In the next chapter, we'll take a look at Backup as a Service (BaaS) in the same manner as this chapter, outlining what it is, who is it best suited for, and when is it the right option for your DR needs.



It's not just about the backup

Purchasing some backup software and cloud storage is simple enough. But when the amount and criticality of the data dictates more than just setting up backup jobs, it's time to bring in a partner with expertise on not just the backups, but on storage management, retrieval, recovery, and optimization of both the backup and recovery of your data.

CyberFortress' team of backup experts have decades of combined experience. Using Veeam Availability Suite, CyberFortress helps to define the specific storage requirements, backup jobs, and data policies to optimize your backups in the cloud.

Protecting Cloud Data:

The Forgotten "as-a-Service"

You've left out an important part of your backup and recovery strategy. With so much emphasis being put on recovering workloads, systems, applications, and data in the cloud, most organizations haven't given much thought to the data that already exists in the cloud.

As part of every organization's digital transformation, the shift includes using cloud-based SaaS applications – such as Microsoft 365, SalesForce, and Adobe Creative Cloud – to handle critical parts of your business operations. Were these same applications available on-premises (as is the case with most of the Microsoft 365 offering), you'd be including the backup of the workloads and data to ensure they can recover. But, because they're online – out there in the ether – most organizations simply cast away concerns for recovering some or all of what makes up these applications.

But you can't. Your recovery strategy – which includes some or all of the services mentioned throughout this ebook – has the singular goal of recovering operations to a known-good state. And, if those operations should include cloud-based applications, you need to incorporate the protection of those applications (to the best of your ability) in your strategy.

For the purposes of this chapter – and given the "aaS" context of this entire ebook – we're going to coin the phrase BSaaS (Backup of Software-as-a-Service, as it were) simply to reference the need and opportunity to protect cloud-applications.

So, what parts of cloud applications can you protect and how should you go about it?

To cover this, we'll use Microsoft 365 throughout this chapter as a model for how you should approach BSaaS.

Defining BSaaS

Every cloud application vendor will tell you they are responsible for maintaining the application - this includes physical security, infrastructure, network controls, and application-level controls. They will also tell you that the data - specifically your data - is not their responsibility to protect. They'll make efforts to maintain it - replication, even backups of data in case they have a service outage - but most (if not all) cloud application vendors are not backing up your data so you can recover it if/when needed.

This view on the separation of duties is so prevalent, Microsoft and other cloud vendors call this the Cloud Shared Responsibility Model. So, in the end, the vendors have the backup of the application covered, but it's your responsibility to ensure your data within their application is backed up and protected. To add this, there is a Service aspect of BSaaS. Many organizations see this kind of backup as "out-of-brand" from their normal backups. Leveraging a partner to define and managed these backups (as part of offering any of the other "aaS" cloud-based options mentioned in this ebook) makes sense.

Based on all this, BSaaS should be defined as the managed backup of cloud application data.

BSaaS as part of your DR Strategy

Most DR strategies resolve around reviving applications and their data - whether initially hosted on-premises or online. And the premise for such a DR strategy is that some unfortunate event (which can be as small as accidental deletion to as big as complete loss of operations) occurs.

In the case of BSaaS there is (in theory) should never be a loss of application; the cloud application vendor should be addressing this. In Microsoft's case, they provide finically-backed services level agreement (SLA) promising 99.9% uptime for most of their services. So, you shouldn't need to worry about the applications. But your DR strategy should take into account the loss of data due to the number of possible factors:

- **Accidental Deletion** – most cloud applications (where deletion by the user is a normal part of the application's use, as in the case of Exchange Online, SharePoint Online, OneDrive, and more) have some sort of deleted item retention. But, should the deletion go unnoticed until well-past the retention time, the only recourse is recovery.

- **Corruption** – While only a handful of cases have been publicly documented, it's still possible for data in the cloud to become corrupted. In Microsoft's case, no backups are maintained, so if a database were to become corrupted, the best they could do is replicate back a known-good copy within their infrastructure, which may include some lost recent changes.

- **Cyberattack** – Cybercriminals attempt to capture user credentials to cloud applications in order to leverage them for spreading malware, data theft, committing fraud, and even to hold the data for ransom. It's the last attack method that is of concern here. A recent demonstration by renowned hacker-turned-security expert, Kevin Mitnik entitled RansomCloud shows how it's possible for Exchange Online mailboxes to be encrypted and held for ransom.

To ensure you DR strategy is comprehensive, every bit of critical data must be included. Data in the cloud is just as susceptible to requiring recovery as it is when on-premises. So, adding BSaaS to your strategy, addressing the specific scenarios outlined above, is a prudent step towards ensuring all of the business can operate.

Who is BSaaS best suited for?

- **Have Critical Data in the Cloud** – If your organization uses a cloud application and relies on that application as a primary means of doing business, BSaaS is an absolute must. For example, if you use Microsoft 365 and email is a primary communications medium between the company and its contractors, partners, vendors, and customers, backing up this data is imperative.

- **Have a Recovery Plan for Everything Else** – Your DR plans cover every server, application, and file system, regardless of whether it lives in the cloud or on-prem. Cloud data, as in the case of Microsoft 365, represents one additional data set that hasn't been included... yet.

- **May Need Some Assistance** – Just because you have a backup of your cloud data, doesn't mean you can do much more than put it back into the same cloud application. But, what if you wanted to take a backup of Exchange Online and recover it to an alternate server for eDiscovery. This is where that Service part of BSaaS comes into play. The actual use of the backed up data may require some outside expertise to assist.

Other Reasons for Cloud Data Protection

Because cloud data is often an afterthought, the idea of protecting it with backups may seem more like an insurance policy than an ongoing DR need. But you backup your data today for more than just disasters.

The desire to migrate the business to a new cloud application requires having copies of the data currently in the old application to migrate with. Mergers and acquisitions also may require the moving of, say, your Microsoft 365 data to either different cloud platform or Microsoft 365 instance. Archives of data may not be possible, or not be as accessible with built-in cloud application features.

BSaaS and Microsoft 365

Microsoft 365 is the most widely used online office application in the world. Organizations relying on it daily need a means to back it up and recover it – whether back into Microsoft 365, or to an alternative destination in order to meet any number of legal, compliance, HR, or business requirements.

CyberFortress uses Veeam Backup for Microsoft 365 as the basis of their managed backup offering to protect your data within Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams. By including this managed service as part of their BaaS, IaaS, and DRaaS offerings, CyberFortress can comprehensively make certain your organization can be put back into an operational state, no matter what the disaster.

What about Cost?

BSaaS normally has no cloud application vendor equivalent, as those vendors are in the business of offering their application, not backups. Usually there are some internal controls that can be used to address simple issues like recovering an item deleted within the last 30 days. But beyond that, leveraging a managed cloud services provider that can offer what we've coined as BSaaS normally incurs costs on a per user, per mailbox, or per instance basis.

Eliminating the Confusion: BSaaS

BSaaS is about utilizing the same partner used for your backup, DR, and cloud infrastructure to define a plan that makes certain your organization's critical lying in cloud applications can be recovered. This gap in your organization's DR plan can be placed in the hands of a trusted provider who ensures recovery of this data is possible.

In our last chapter, we'll take a look at all of the service offerings mentioned in this ebook and provide guidance on how to choose the one that's right for your organization.

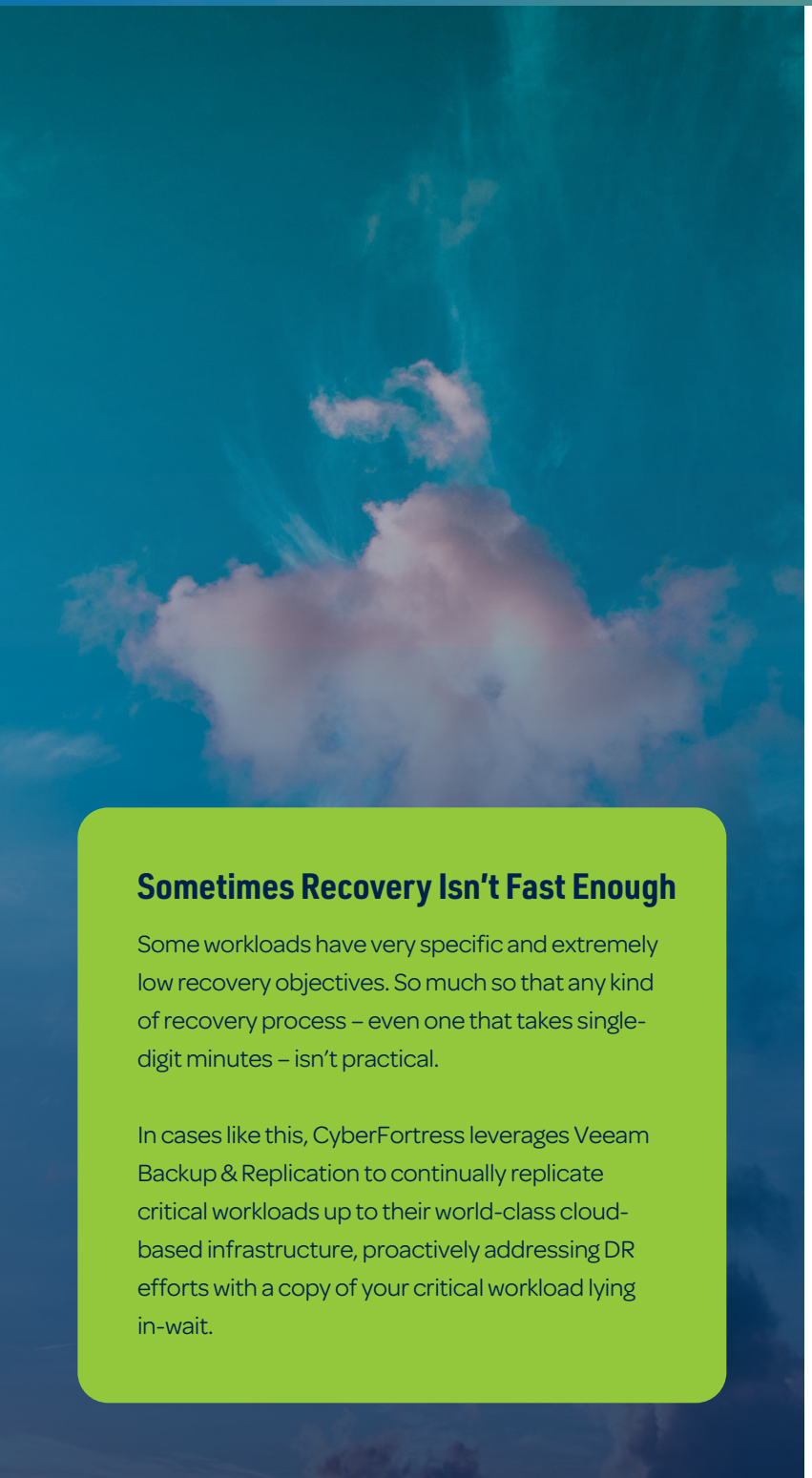
Choosing the Right Service:

Meeting Your Disaster Recovery Needs

The success or failure of a recovery rests solely on whether Over the last four chapters, we've introduced you to – and educated you on – four of the most common services offered around disaster recovery. After reading all four chapters, it may be a surprise to you, but some of you may find that more than one service could be used to meet your needs. Are you supposed to choose just one? Would that even work for you? It might be that, at this point in the ebook, you're a bit more confused than when you started.

And that's what this chapter is all about.

In this chapter, we'll take a look at why each service is a viable choice, provide a comparison among them, and then cover some of the considerations when choosing the right provider.



Sometimes Recovery Isn't Fast Enough

Some workloads have very specific and extremely low recovery objectives. So much so that any kind of recovery process – even one that takes single-digit minutes – isn't practical.

In cases like this, CyberFortress leverages Veeam Backup & Replication to continually replicate critical workloads up to their world-class cloud-based infrastructure, proactively addressing DR efforts with a copy of your critical workload lying in-wait.

Why BaaS?

Many organizations will choose Backup as a Service because it has the lowest barrier to entry. Unlike IaaS or DRaaS (where a significant investment in planning and implementation is necessary to get the service properly configured), BaaS requires little more than the installation of backup software locally and the definition of backup jobs to get started. If you're more concerned with having managed offsite backups of your data and plan on addressing DR if and when it becomes necessary, Baas is for you.

Why IaaS?

Organizations wanting to proactively host critical workloads in the cloud while managing it themselves choose IaaS. The value to your DR strategy is that these workloads are already running offsite in one of the safest and highly available data centers in the world. The upside for internal IT is the retaining of control over the entire environment – without having to invest in your own SuperNAP. But it's a double-edged sword – in theory, the use of IaaS should offset a material amount of risk, but should the disaster be the corruption of a database on a server hosted in IaaS, it's all on internal IT to rectify the problem.

Why DRaaS?

Most organizations have at least one critical workload they simply can't live without - when all hell breaks loose. And, in your time of need, you simply want to know someone is working diligently to restore service to your employees and customers. Whether a single workload, your entire network, or something in between, DRaaS provides organizations with the confidence that, no matter the disaster, the designated workloads will be up in the time-frame promised, minimizing the damage caused by disaster.

Comparing Services

Use the considerations in the following table to identify the right service to help you with your DR needs.

Rating System

0 1 2 3 4

Worst/Least Best/Most

Consideration	BaaS	IaaS	DRaaS
Organizational			
Focus	Backup	Operations	Recovery
Typical Workloads	All	Critical	Critical
Can Include Everything?	4	4	4
Good for Regulation Industries	2	2	4
Hosted Worldwide?	4	4	4
TCO	$	$$	$$$
IT-Centric			
IT Involvement	2	4	2
Visibility	2	4	2
Control	2	4	2
Physical Security?	4	4	4
Network Security?	4	2	4
Use for Encryption?	4	0	4
Planning Required	2	3	4
Recovery-Centric			
Proactivity	2	4	3
Responsiveness	Hours	Already Up	Minutes
Testing	0	0	4

Why Backup Cloud Data?

In addition to protecting your operationally environment with BaaS, IaaS, and DRaaS, you also rely on cloud applications like Microsoft 365 – which makes it part of operations and, therefore, part of your data protection strategy. So, rather than thinking about this as fitting into the mix of "which one is right for you", this issue sits firmly in the "and you need to do this as well" category. It's your data; protect it.

Choosing the Right Provider

By now, you should have a better idea of which service(s) are right for your organization. But, with so many cloud providers vying for your business, how do you select the right one? The most critical aspect of the selection process is to ensure you are considering the needs of the organization, determining whether the provider meets those needs.

So, the following non-exhaustive list of criteria are much more about your organization's need, than they are features of any given provider. Use the following considerations to build a "must-have" list when searching for a service provider.

- **Market Specialization** – Is your organization in an industry vertical that must meet specific compliance standards or certifications? If so, your service provider should specialize in helping organizations like yours, ensuring you maintain adherence your industry's mandates.
- **Geography** – Does your organization have particular requirements regarding where data, systems, and applications are to be hosted?
- **Hosting Model** – Do you want your workloads stored in a public cloud - Object Storage, a collocation, or the provider's facilities?
- **Data Center Architecture** – What kind of hardware does your applications need to run on? Is the data center designed for with security, redundancy, and sustainability in mind? Is the hardware designed for data center use? Is it commodity hardware?
- **DR Services Offered** – Of the services you identified using the table on page 27, are they offered by a given provider?
- **Service Levels** – What are your requirements around service levels from a performance, availability, and recoverability standpoint for each workload involved? Consider these in conjunction with the provider's hosting model to identify if there are any dependencies that may make meeting service levels difficult.
- **Recovery Objectives** – What are your per-workload Recovery Time and Recovery Point Objectives? Despite offering the services you need, can the provider meet (and exceed) your recovery objectives?
- **Pricing Model** – What kind of cost structure best fits your organization? Does it need to be entirely an operating expense? Can some capital expense be incurred, if necessary? What kind of budget is available for DR, and can the allotted budget grow over time?

Making the right choice

You started this ebook with some level of confusion around which "aaS" would be right for your organization's DR needs. By understanding each of the services offered, what they bring to the DR table, and how they will be used to keep your business running, you can align your own business requirements with the appropriate services. This not only clears up the confusion, but also empowers you to form the foundation for creating a new cloud-based DR strategy, complete with a seasoned provider that will work to help you meet your recovery objectives.

Finding the Right Mix of Provider

While all there are many considerations that can help point to a potential provider, your "aaS" requirements may dictate that simple commodity offerings won't do the job. The right provider should also offer blend of services, support, software, and infrastructure can tailor the offering to meet your specific needs.

CyberFortress focuses on providing the necessary cloud services and Veeam solutions, meeting clients at their point of need, delivering custom offerings that meet customer's need – both now and in the future.

Conclusion

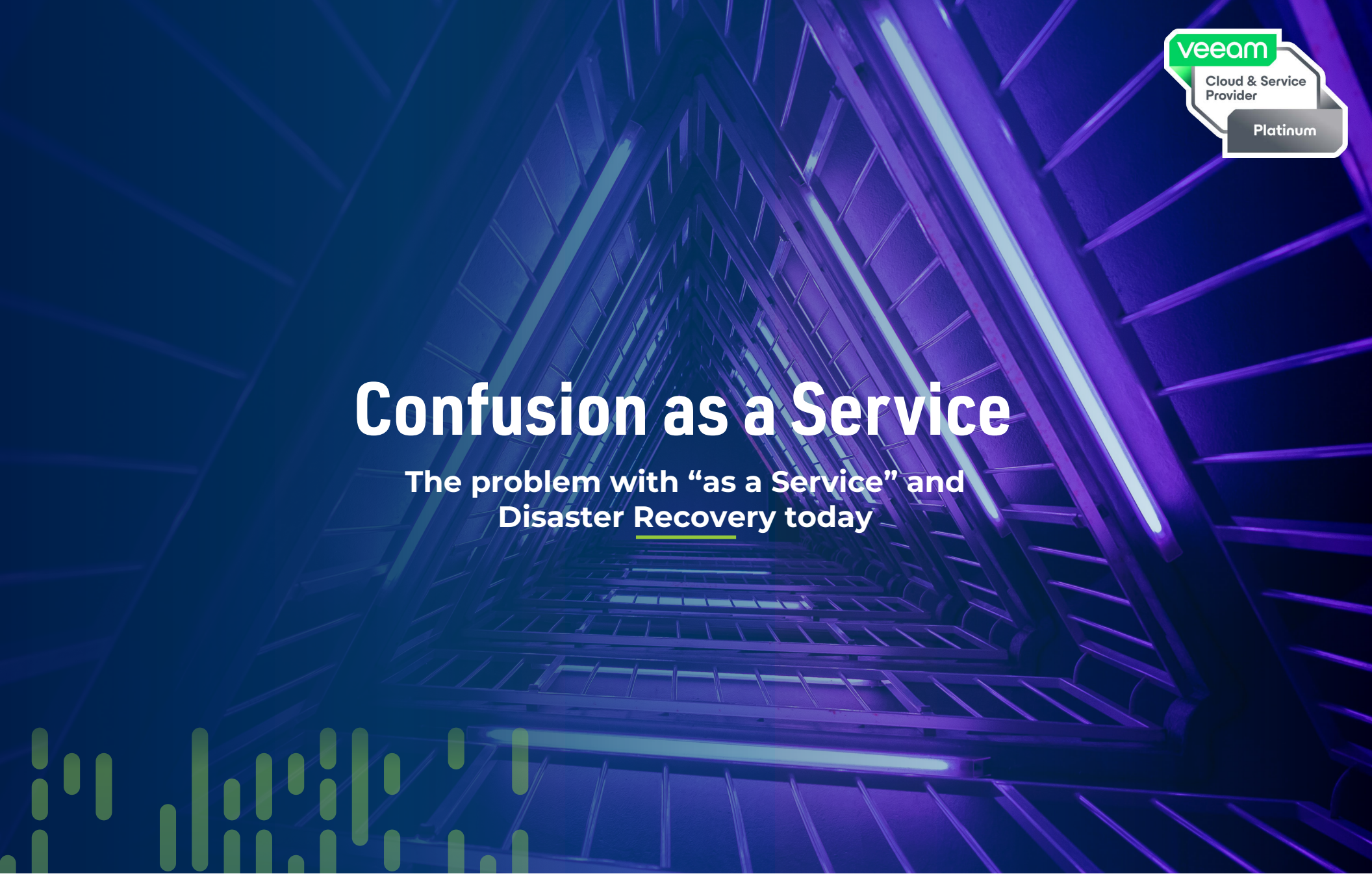
Clearing Up The Confusion: Right Service, Right Provider

It is possible to clear up the confusion around DR and the myriad of "aaS" offerings today. The 5 chapters in this ebook were designed and presented in a way that allows you to both understand the services you should consider, and – more importantly – see your own organization's need. The answer lies at the intersection of the two.

By actionably identifying your organization's DR needs – on a per-workload basis – and then identifying the appropriate service that will maintain the workloads availability, it becomes a simple task of finding the right provider. So simple, that it no longer will be a discussion around "what do you offer?", but instead one around "I have these needs. Can you meet them and have you done this before?"

See the difference?

1. **Identify your workloads**
2. **Determine your Recovery Objectives for each**
3. **Clarify any other requirements (e.g. geography, compliance, etc.)**
4. **Establish which DR-related services best meet the need (per workload)**
5. **Build a requirements list from steps 1-3**
6. **Vet providers by presenting your requirements**



Confusion as a Service

The problem with “as a Service” and Disaster Recovery today

CyberFortress™
The Recovery People

cyberfortress.com
855-223-9322
sales@cyberfortress.com