comport

TECHNOLOGY SOLUTIONS | HEALTHCARE SOLUTIONS

Modern Data Protection: Why Backup Alone is not Enough.

The Show Must Go On

With few exceptions organizations today are highly Data Dependent. Tolerance for outages of any kind, even during or after a major disaster, is very brief indeed. In fact, according to an ESG survey, 35% of servers in enterprises have a recovery goal of less than 15 minutes. Customers and Internal End Users expect technology to be up and running quickly in the event of an outage – ideally, they never notice you went down. They trust that the IT department has strong processes and procedures that ensure they can carry on no matter the circumstance.

Today's data consumption models pose new challenges for data protection, data can be housed in public, private, or hybrid clouds. To add to this complexity, end users are much more reliant on SaaS applications, such as Salesforce, Microsoft Office 365, SharePoint, and even OneDrive which are frequently not protected by backups or DR. Also added to the mix are the new demands to protect data that doesn't live "onsite" such as data stored on laptops, smartphones, and tablets. Technology teams must find a way to backup and protect their data, no matter the location.

Data protection is no longer about securing your on-premises environment, but about securing ALL your data by ensuring proper backup and disaster recovery strategies. This has produced solutions that may require on-premise backups, Backup as a Service (BaaS) and replication or Disaster Recovery as a Service (DRaaS) as the right combination to meet your goals. Companies must now be proactive rather than reactive, putting in place, high-availability and failover technologies for their data.

When looking at the continuum of data protection, companies have traditionally focused on firewalls, network, and endpoint protection to ensure their data is safe. While threat prevention is still important, companies must understand that threats are evolving at a very rapid pace and, despite their best efforts, it's not a matter of if but when they will have a breach. By 2019, despite the increasing effectiveness of countermeasures, we can expect 3 million successful ransomware attacks, up from 2 million in 2016. Because of this, there is a trend towards organizations who are adopting comprehensive backup and disaster recovery strategies.

When it comes to preparing for a disaster, you can never be too careful – or too prepared.

What is Disaster Recovery as a Service (DRaaS)?

Disaster recovery as a service (DRaaS) uses the cloud to backup your environment, protecting your applications and data from any disruptions caused by disaster. For a true, rapid restoration in the event of a disaster you must have both frequent backups and continuous transference (replication) of critical virtual machines. DraaS gives an organization a total system backup that allows for business continuity in the event of system failure.

Disaster Recovery as a Service (DRaaS) presents businesses with an opportunity for an efficient, cost-effective data strategy because DRaaS utilizes the cloud, allowing scalable replication to as many VM's, databases, storage systems, and sites as you need, regardless of storage, applications and operating systems. In addition, the cost of a DRaaS allows companies that couldn't afford to build or lease a secondary data center with a feasible option for recovery.

The Right Protection for Mission Critical Data

IT downtime comes with a hefty price tag. If you were to ask an organization if they were protected from an outage, most would say "yes" based on the fact that they have multiple copies of their data. What defines the resilience of a company, however, is not the amount of data protected but the availability of that data. To successfully restore your data, you need to have a place and an environment where the data can reside and be accessed from.

So, what happens if you sustain a disaster — be it a natural disaster or a cybersecurity attack? Unlike a backup environment that houses your data, a Disaster Recovery environment replicates your entire computing environment (data, systems, networks, and applications) to create a complete business continuity plan.

Are you sure you're protected in the event of an outage? Here are some questions to ask yourself.

To check the likelihood that what you consider your Disaster Recovery Solution will be successful, ask if it fulfills the following:

1. Can the environment be restored within the required RPO and RTO?
2. Can you restore applications and systems, not just the data?
3. Can critical business operations be carried out for a prolonged period of time in the DR environment?
4. Do backups continue to run in your DR environment?
5. Do you have the expertise on your staff to get you up and running if something fails during an outage?

By using a DRaaS service provider, organizations can backup their data and fully restore applications, data, and system images (virtual and physical) from the cloud, which provides a quicker path to restoring business operations. Leveraging a respected BaaS and DRaaS provider for day to day protection also provides an added layer of assurance that you will have experts at your fingertips in case of an outage for assistance when you need them.

What exactly are the benefits of Disaster Recovery as a Service?

Benefits of DRaaS

In IT, the only certainties are bugs and outages. Disasters may seem unlikely, but they occur with increasing frequency and can pack a punch. Disasters with prolonged outages threaten reputation, financials, jobs and the very survival of the organization. Without a well-conceived DR plan, IT specifically is vulnerable to corporate and board-level scrutiny. DRaaS is adopted more and more because it perfectly checks so many boxes.

Security

A DRaaS solution protects from cybersecurity attacks by providing an air gap between infected backups and a clean replication to restore from. One of the issues of having all copies on site is that the attack can affect all internal copies, even if they aren't directly connected.

Availability

Improving availability is the main business driver for DraaS, whether a single VM or an entire environment. Extending your existing data center to the cloud significantly improves the availability of your critical applications.

Pay as you Go: From Capex to Opex

Prior to DRaaS, the best disaster recovery options involved major up-front capital investments, with complex architectures and expert staff to manage and maintain the environment. Feature for feature, implementing DRaaS creates a superior TCO over traditional disaster recovery.

You no longer need to make huge capital outlays, in most cases you can leverage your current environment — simply pay for your current resource allocation, month by month (or if you choose yearly). DRaaS can ensure better, affordable protection for any business.

Simplicity

A DRaaS solution provides all the elements of a duplicated data center environment such as disaster recovery site planning, architecture, and capabilities, without the complexity. Traditionally, this type of solution required expensive tools and systems, that often needed custom integrations to work together. With DRaaS, you have the system you need with the expert staff just a phone call away.

360 Visibility

Because you'll have a single GUI for your BaaS and DRaaS solution, you get a full-circle view of what's going on in your environment, with the flexibility to add VM's or physical machines instantly. You'll have full visibility into your data backups and replications with updates on the state of your VM replications and managed servers (whether they are processing workloads or in failover).

Scalability & Flexibility

DRaaS solutions scale upward and onward to cover as many VMs, databases, storage systems, and sites as your organization requires. With DRaaS, your DR environment grows as you do, ensuring that resources are dynamic. You can easily confirm that you have enough network bandwidth for moving data, enough servers for your VMs, and enough primary storage for your jobs. In addition, DRaaS solutions are technology agnostic, which means you have tremendous flexibility in terms of mixing and matching operating systems, virtualization platforms, database management systems, and backup tools.

DR Testing on Demand

Before DRaaS, conducting DR testing was more difficult, time consuming, and risky - often resulting in production systems going offline. DRaaS has automated management of virtual machines, backups, and replication making testing failovers as simple as point and click.

Compliance

DRaaS helps organizations with their compliance requirements by providing the controls needed to monitor and protect critical and sensitive information. You'll be able to show your auditors and regulators where your data is located and who has control over it, through a single pane of glass.

Competitive Advantage & Survival

How could DRaaS help with a competitive advantage? You now have one reliable vendor who is ensuring that your business will be there for you and your customers in the future. Ask yourself this, in the event of a disaster, are you positive you can get back up and running without help? Without DRaaS, you are placing your bet that a natural or cybersecurity breach is not going to happen to you. DRaaS enables organizations of any size to plan for the worst - and feel confident they can focus on their day to day business.

Things to Think About when Selecting a DRaaS Provider

Data Center Location

Consider a partner that offers proximity, but not so close that they may be affected by the same disaster, or so far away that the latency and network bandwidth negatively impacts the ability to recover within the terms of the SLA. Some organizations spread the risk, for example with a provider that has both east and west coast facilities.

Capabilities

How does the DRaaS provider handle mixed environments? If you have a mix of physical, virtual, and cloud servers, each with different SLA levels — can they handle different RTOs? Do they include regular testing as part of their service? Does their testing interrupt production environments? How is the testing performed? What reports can they provide? How frequently? Do they have deep technical capabilities both in data protection and the underlying compute and storage systems technologies? What kind of data center do they use to store your images and data? What are the security provisions?

DR Readiness Assessments

Environments grow and change over time. It can be helpful for experts to analyze needs and make DR recommendations, and deliver or update your formal Disaster Recovery Plan. Many details involving tiering and other factors can present unforeseen problems down the road, if not understood upfront. Does your vendor offer this?

Level of Attention & Financial Viability

The choice of your DRaaS provider is very important – this is your partner in an area vital to your business. Not only is it important to understand capabilities and location so they align well with your needs, but it's also important to know they are financially sound. Ask the question: Will the provider be around to restore you in the event of a real disaster? Can they provide your company with the personal attention you may need when you are upset and faced with a major problem?

The Disaster Recovery as a Service (DRaaS) market size is expected to grow 41.8% by 2022.[2]

Wrapping it All Together

Most organizations today have a variety of IT infrastructures to protect: physical, virtual, and cloud hosts. It's critical to have a business continuity plan that includes backup and disaster recovery strategies that simplify protection of your complex environments. Using an appropriate combination of traditional backup (tape and flash storage) and BaaS in conjunction with DRaaS provides an easier, cost-effective solution for safe data management and recovery. Organizations that implement these strategies enjoy the benefits of simplified backup and recovery administration, reduced costs, and protection from cyber threats.

ComportSecure

If you are a Veeam customer, or are considering Veeam, ComportSecure BaaS and DRaaS solutions work hand-in-hand with Veeam's Availability Suite. ComportSecure Disaster Recovery as a Service takes advantage of your existing or planned investment in Veeam backup. A simple technical integration with ComportSecure sets up your replication jobs; there is no need to acquire, learn or maintain additional technology. Veeam Cloud Connect encapsulates and encrypts all network traffic for management, replication and even inter-VM communication. No VPN connections or open firewall ports are necessary.

ComportSecure specializes in disaster recovery planning and implementation with Recovery Time Objectives (RTOs) significantly less than 15 minutes. Clients can fully failover to replicated VMs or partially failover to ComportSecure's secure compute infrastructure. Failback can be to the original location or to new infrastructure. Replication is scalable to as many VMs, databases, storage systems, and sites as you need, regardless of vendor.

Contact Comport today to learn more about our backup and disaster recovery solutions.

[1] Solutions Review "Backup and Recovery Statistics You Should Know Before 2018", November 22, 2017

[2] Markets and Markets "Disaster Recovery as a Service Market worth 12.54 Billion USD by 2022"

comport

TECHNOLOGY SOLUTIONS | HEALTHCARE SOLUTIONS

New York Area Office
78 Orchard Street
Ramsey, NJ 07446
Phone: (800)830-0330

New England Office
100 Federal Street
Boston, MA 02110
Phone:(800)830-0330

Mid Atlantic Office
1735 Market Street
Philadelphia, PA 19103
Phone: (800)830-0330

Hewlett Packard Enterprise
Platinum Partner

Hewlett Packard Enterprise specializations include Platinum: Converged Infrastructure.

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.