StorageCraft

Always Safe, Always Accessible, Always Optimized

www.StorageCraft.com

Disaster Recovery Cloud:

NOT ALL CLOUDS ARE CREATED EQUAL

Your Technology Partner for Business Continuity

StorageCraft

Always Safe, Always Accessible, Always Optimized

1

For end-to-end business continuity, organizations need next-generation data protection. Here's an inside look at how to provide the right disaster recovery cloud solution for you and your customers.

With the phenomenal growth of cloud computing, more and more organizations are leveraging cloud-based solutions for all their business needs, including options for cloud-based disaster recovery (DR). Companies are moving to public, private, and hybrid cloud in large numbers for a variety of use cases, including disaster recovery. While these companies are well versed in managing hybrid clouds, the success criteria for cloud-based disaster recovery is not the same. Disaster Recovery as a Service (DRaaS) is different.

This gap in understanding is of particular importance to Managed Service Providers (MSPs)—as it spells opportunity for solution providers who have the expertise and product line partnerships to provide cost-effective disaster recovery solutions. Whether your customer operates in retail, healthcare, finance, government, or education, each of them could benefit from establishing cloud-based data protection services.

A key selling point is that when built correctly, cloud-based DR can dramatically reduce downtime. Businesses are very aware that downtime has a negative impact not only on employee productivity, but on customer experience. The big effect of downtime is of course on revenue, and the numbers are eye-popping. Gartner estimates that downtime can cost a company $5,600 per minute, which is $300,000+ per hour.*

As a qualified expert with an arsenal of offsite data protection options, you need to have the expertise to build an intelligent, cloud-based disaster recovery platform that offers your customers total business continuity. A disaster recovery cloud can provide 99.999+ percent uptime for customers, which is a number they will surely appreciate.

Ready to become a disaster recovery cloud expert? Let's take a closer look at four key areas:

1. The market opportunity for DRaaS
2. Why you need to use a cloud that is purpose-built for disaster recovery
3. The security considerations of cloud-based DR
4. The cost advantages of pooling cloud services

StorageCraft

Always Safe, Always Accessible, Always Optimized

2

Tapping into the DRaaS Opportunity

As you probably know, cloud computing continues to advance in every aspect of business, for companies large and small. Worldwide spending on public cloud services and infrastructure hit $160 billion in 2018, according to IDC. One increasingly popular application of cloud computing is for offsite data protection and backup. Cloud-based disaster recovery can improve the resilience of entire IT systems in the case of a disaster due to a malware attack or created by human nature or Mother Nature.

Simply put, the DRaaS model protects applications and data from disruption caused by disaster. It provides an organization a total system backup that allows for business continuity in the event of system failure. With DRaaS, you can reduce the time to return your customer's applications to production. DRaaS can be especially useful for your small and medium-sized customers that lack the necessary expertise to provision, configure, and test an effective disaster recovery plan.

Growth in this area to date is noteworthy, as Gartner reports that DRaaS worldwide revenue was $2.4 billion in 2018 and will grow to $3.7 billion by 2022, with more than 500 providers. The strongest growth is in smaller enterprises, with more recent growth in enterprises with 1,000 to 5,000+ employees.** Gartner also notes that in 2018, the number of organizations using cloud-based disaster recovery or the DRaaS model exceeded the number of organizations using traditional recovery services.

StorageCraft

Always Safe, Always Accessible, Always Optimized

3

Public Cloud Platform Growth

Most of your customers may already have cloud-based services from one of the big public cloud providers, such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform. Customer demand for the public cloud means growth in cloud-based services is continuing at a dramatic rate.

According to a recent IPED Consulting research, AWS has experienced 47 percent growth, Microsoft Azure has grown 91 percent, and Google Cloud saw double-digit growth. That same research notes that solution providers should be prepared for even more growth in the next six months.

Solution Providers See Demand for Public Cloud Services

Source: IPED Consulting & The Channel Company

Your job is to educate your customers on the optimal cloud strategy for their business, including what applications might require a cloud purpose-built for data recovery. There is no "one right answer" when it comes to multi-cloud vs. dedicated cloud strategy.

Typically, a multi-cloud strategy is the approach most businesses prefer. You can capitalize on that opportunity by knowing the pros and cons of having some applications in the public cloud, while others—such as disaster recovery and backup—reside in a cloud built specifically for disaster recovery.

StorageCraft

Always Safe, Always Accessible, Always Optimized

4

A Purpose-Built Cloud

Your customers may not know why they need a different type of cloud service to facilitate their recovery efforts. In fact, some data management companies even talk about how ANY third-party cloud can suffice as a data backup solution. This sometimes means the business sets up just a copy of all their data in the public cloud.

While that may (partially) help the business in the event of a disaster, it isn't a true recovery solution. The ability to easily, fully, and cost-effectively recover a customer's data—rapidly—requires the use of a purpose-built disaster recovery cloud. The reason: Not all clouds are created equal.

Let's take a look at how a public cloud is different from a cloud purpose-built for recovery, and how those differences come into play after a disaster event. Companies today tend to have "cloud sprawl" and multiple unconnected data silos, where different applications, data, and management tools may be running in the public cloud, partially onsite, in a hybrid cloud, and/or in a private cloud. These mixed configurations can be extremely difficult to manage, especially during a disaster.

Public clouds work much like a parking lot for data—where it's easy to put data in and get it back down. But once you need to do anything to the data or access specific parts, the system gets complex. When choosing a cloud for disaster recovery, take a close look at the cost structure and the accompanying pay-as-you-use fee system. For example, most public cloud services providers charge a fee, both for data being ingested (entering their datacenter) and for data upon egress (exiting their datacenter).

Also note that a distributed, multi-vendor cloud architecture doesn't provide a single pane of glass view of all the data at an organization. Without that, getting the company up and running again after a disaster may take hours, or even days, to piece together all the critical information needed for total business continuity. Think back to the parking lot example, where trying to locate where your car is parked in a sprawling, crowded lot always takes more time than you anticipate.

StorageCraft

Always Safe, Always Accessible, Always Optimized

5

Recover Data and Virtual Machines in Minutes

With a cloud purpose-built for disaster recovery, you have a single view of your customer's resources, and you can provide protection for all of its on-premises business systems and data. By offering integrated cloud services, you will help them recover data and compute and network services, all in an orchestrated recovery workflow.

That means that in the event of a major disaster, you can quickly get your customer's critical operations running again. With a cloud service designed for data protection, you can recover data, virtual machines, or even fail over an entire customer site and network in minutes. This is impossible if your customer has a sprawling, multi-vendor cloud configuration that doesn't provide a single view of all the data and applications that need to be recovered.

Another best practice in disaster recovery cloud strategy is to utilize technology that gives you the capability to centrally manage backup and recovery through an online portal. You need to have visibility and access to all of your customer's stored backup images. By maintaining control over networking, you can then offer your customer seamless failover during a disaster.

Focusing on Security

A top consideration in any disaster recovery strategy is maintaining a keen focus on security. Your cloud-based DR solution should allow you to provide your customer top-tier, military-grade security (SSAE 16 certified, AES-256 encryption).

It should also protect your customer from attacks and malware. With the right DRaaS, a business can survive anything, including the all-too-common ransomware attacks that are occurring in many industries, and especially in healthcare. In fact, statistics from insurance company Beazley show that healthcare firms file more ransomware claims than any other industry. ***

With cloud services, you can replicate backups to the cloud, where encrypting malware can't reach them. And in the case of an attack, you can quickly retrieve data, virtualize machines, and re-create your customer's network with a customized cloud configuration.

StorageCraft

Always Safe, Always Accessible, Always Optimized

6

Industry Profile: Healthcare

Medical data comes in various formats including clinical notes, diagnostic tests, genome sequencing, and medical images. The massive growth in imaging volumes and file sizes has placed an immense burden on storage requirements. It's no surprise that healthcare IT teams are constantly challenged to balance capacity planning and storage costs.

But while business continuity is always important, it's crucial for healthcare organizations. CIOs are under intense scrutiny because of the sensitive nature of data, while at the same time, their organizations are under pressure to reduce the financial impact of downtime. Loss of data availability and downtime can occur in several ways, from accidental file deletion, hardware failure, ransomware, to natural disasters. Hospitals are especially vulnerable to ransomware attacks and they are the number one target for cybercriminals.

Solution: StorageCraft eliminates hospitals' runaway storage costs and reduces data management complexity. The OneXafe™ product family is a unique scale-out, object-based NAS storage appliance. It can be utilized as primary data storage, archiving (e.g., medical image repository), and a target for backups.

Benefits: For healthcare organizations, a solution provider can have a purpose-built disaster recovery infrastructure installed and replicating. The solution will protect the organization against costly downtime and ransomware attacks.

Find out how the StorageCraft Partner Success Program can help you optimize your recurring revenue efforts. Enrollment is FREE. Visit: www.StorageCraft.com/Partners

Become a StorageCraft Partner

CLICK

StorageCraft

Always Safe, Always Accessible, Always Optimized

7

The Cost Advantages of Pooling Cloud Services

One important topic to discuss with your customer is how cloud-based DR compares to traditional on-site backup and disaster recovery. For the business, building out its own data center for disaster recovery is costly. Because the business is only billed for storage in use, the spend on DR resources can be substantially less than if the business purchased hardware, space, and hired tech staff to run an entire second datacenter 24x7.

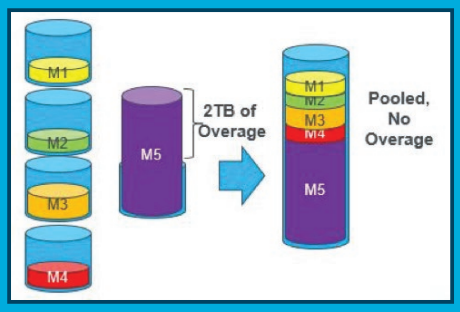
Providing cloud-based DR services can also be cost-effective for you—if you choose the right cloud services partner. When you look for cloud services for disaster recovery, consider a partnership that offers storage pooling among your customer base. This will eliminate wasteful spending on cloud storage that is not being used. With storage pooling, each machine's allotted data storage of 1 TB will be pooled across all machines with a service provider's account, based on a service level.

Here's an example of how pooling with StorageCraft Cloud Services works. Note that pooling is done at the MSP level, with pools at each Service Level (Cloud Basic, Cloud Plus, and Cloud Premium).

Example: A customer has five machines in Cloud Services Premium.

Machine sizes: M1= 300GB, M2 = 250GB, M3 = 500GB, M4 = 300GB, M5 = 3TB

Total capacity = 4.35TB



The StorageCraft Cloud Services licensing model lets you take advantage of pooling, offering this set of benefits:

- Per machine per month pricing
- 1TB of capacity per machine
- 30 days a year of virtualization included
- Expedited BMR drives

You can quickly see that cloud services that allow you to pool customers can result in cost savings vs. having to pay for unnecessary storage overage.

Next Steps

If you are ready to dive into the lucrative data protection opportunities in cloud services and DRaaS, learn more about the advantages of partnering with StorageCraft. With StorageCraft Cloud Services, you can protect your customer's on-premises business systems and data in a cloud that is purpose-built for total business continuity.
StorageCraft has a full suite of products that allow you to bring a comprehensive, price-competitive disaster recovery solution to business customers that will add new revenue streams and differentiate you from the competition.

Learn more: **https://www.storagecraft.com/join-partner-success-program**

Footnotes

*Lerner, Andrew. "The Cost of Downtime." Gartner Blog Network, 16 July 2014, blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

** Panetta, Kasey. "5 Strategic Technologies on the Gartner Hype Cycle for Midsize Enterprises, 2018." Smarter With Gartner, 27 Sept. 2018, www.gartner.com/smarterwithgartner/5-strategic-technologies-on-the-gartner-hype-cycle-for-midsize-enterprises-2018/

*** "Beazley Breach Insights - October 2018." Beazley, 1 Nov. 2018, www.beazley.com/news/2018/beazley_breach_insights_october_2018.html