Best Practices to Leverage the Cloud for Disaster Recovery

Written by Chris Patterson
Senior Director, Product Management

75%

Of companies do not have a disaster recovery plan

25%

Of companies do not recover from catastrophic disasters

Modern IT and computing infrastructure have grown beyond the typical on-premises physical and virtual hardware in data centers to more complex hybrid architectures. As a result, the associated disaster recovery (DR) implementations of tapes, disks or SAN-to-SAN replication have become more complex and expensive. Lowering risk and ensuring business continuity in the face of a disaster has become daunting for organizations of all sizes.

A study by Nationwide Insurance found that 75 percent of business owners don't have a disaster recovery plan, even though 52 percent stated that average disaster recovery time can take as long as three months. Among organizations that do not have a DR plan, 25 percent do not recover from catastrophic disasters. These statistics suggest that organizations should invest in a good disaster recovery solution to protect business-critical data and applications in case of a disaster.

75% of organizations don't have a DR plan

Average of 3 hours for recovery from disasters

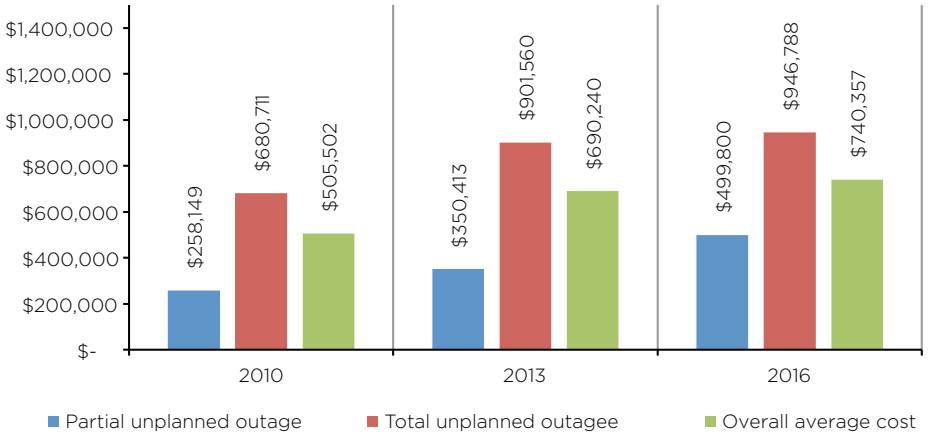
25% of businesses do not recover from a disaster

Source: Nationwide Insurance survey of 502 businesses, June 2016

"The cost of an outage has increased dramatically in recent years."

Ponemon Institute

According to a study sponsored by Vertiv on the datacenter outages at companies across different industries, the cost of an outage has also increased considerably over past few years.



Source: "Cost of Data Center Outages," study by the Ponemon Institute and sponsored by Vertiv.

The cloud is revolutionizing many aspects of IT and Disaster Recovery, and is very often cited as one of the first and easiest ways an organization can take advantage of cloud computing. In fact, cloud-based Disaster Recovery as a Service (DRaaS) has grown by leaps and bounds in the past couple of years. That's because it has a significant competitive edge over traditional DR solutions in ease of configuration, consumption, and management. According to a study by research firm MarketsandMarkets, the DRaaS market is expected

$12.45B

Expected size of DRaaS market by 2022

42%

Compounded Annual Growth Rate from 2016 to 2022

to reach $12.54 billion by 2022, from $1.72 billion in 2016. This reflects a compounded annual growth rate (CAGR) of 42 percent.

The pay-as-you-go model associated with cloud service is another key benefit that attracts organizations to explore DRaaS as a serious option in their business continuity plans.

This study will explore the evolution of DR solutions, the value proposition of cloud-based DRaaS options, and the recommended best practices when leveraging the cloud for Disaster Recovery.

ADDRESSING BUSINESS CONTINUITY CHALLENGES

Planning for business continuity involves addressing several challenges faced by organizations. These challenges include data and application complexity, exponential data growth, long-term retention and media management, different needs of different business units, untested DR plans, dealing with the effects of ransomware, and more. Below is a brief explanation of each of the various challenges.

DATA AND APPLICATION COMPLEXITY

Interdependency of applications, complexity of data management, and change control make it difficult to establish procedures for business continuity. Even if there is defined business continuity plan, many organizations find the plan difficult to adhere to because of implementation difficulties. An ideal DRaaS solution should be able to manage the interdependencies, and provide a seamless implementation experience.

EXPONENTIAL DATA GROWTH

"Data growth rate is averaging 40% per year"

IDC

Data growth rate of organizations is averaged at 40% a year as per a study conducted by IDC. This study states that the data size in the digital universe will reach ranges of 44 trillion Gigabytes by 2020. When data size increases, backup and protection costs also increase exponentially. This frequently forces organizations to focus on protecting their most critical applications, while leaving the less critical applications with minimal or no protection. DRaaS solutions leverage cloud storage and can scale as needed to handle growing data size.

LONG-TERM RETENTION AND MEDIA MANAGEMENT

Long-term retention of backup data sometimes becomes necessary due to compliance or regulatory requirements. The logistics of long-term data retention are challenging because it requires an efficient mechanism for media management. To enable long-term data retention, backed-up media must also remain usable without any physical damage. Cloud-based DRaaS makes this task easy. The stored media in DRaaS resides in the cloud and is managed by a service provider, with guaranteed long-term retention agreements.

BUSINESS-UNIT SPECIFIC REQUIREMENTS

Depending on the importance of the applications they use, different business units in the same organization can have different DR requirements, RPOs and RTOs and budgets. The DRaaS solution should be versatile enough to

accommodate these requirements, including the ability to support varying RPOs and RTOs for different workloads.

DR DRILLS

A well-documented DR plan does not always guarantee a flawless recovery in the event of a disaster. To avoid last minute surprises, DR plans should be tested periodically to identify and resolve obstacles and challenges. Ideally, a DRaaS vendor should be able to facilitate risk-free DR drills, without requiring any downtime for production environments.

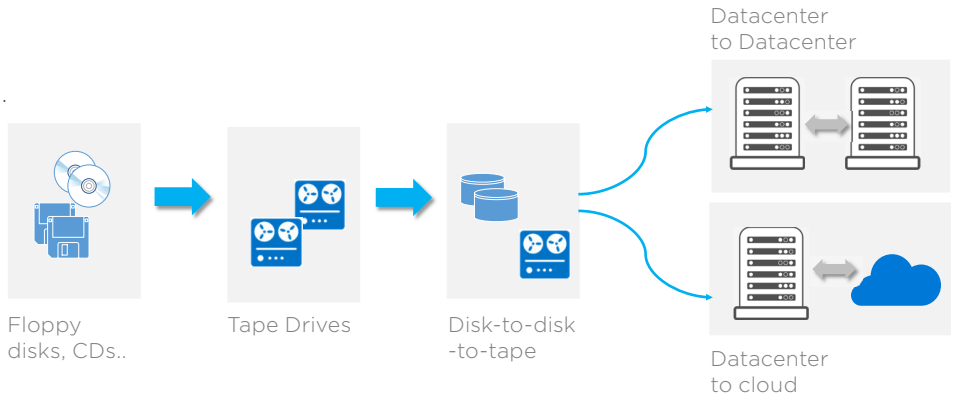
EVOLUTION OF DR SOLUTIONS

DR solutions have come a long way from tape- and disk-based backups. What used to be periodic backup and offsite storage has evolved into real-time continuous data replication, point-in-time snapshots, and hybrid recovery solutions. Magnetic tape-based recovery options dominated for a long time before giving way to disk-to-disk-to-tape solutions. Storage of data in disks provided a quick recovery option if organizations didn't need to retrieve tape from a distant offsite storage location. This offsite facility could be managed in house by the organization, or by an external service provider contracted according to proper SLAs.

The concept of offsite data storage is critical in that many organizations are required to have a copy of data in a safe, geographically distant location in the event of a catastrophe at the primary data center. This element of a good DR solution is still valid in modern-day DRaaS offerings. But instead of relying on a physical offsite shipping process, DRaaS solutions use secure networks and cloud-based storage. Data is stored securely in your cloud service provider data center, with replication options to multiple locations. That means, even in the case of a disaster affecting a specific location, you can still recover applications and data from the locations where the replicated data resides. Storage-level replication of data to an alternate data center is popular with organizations that do not want to send data to the cloud because of regulatory or compliance requirements. Virtualized environments can use native asynchronous or synchronous replication capabilities offered by SAN storage vendors. Environments with no investments in SAN can go for technologies like Hyper-V replica, Stretched clusters etc.

"DR solutions have evolved into real time continuous data replication, point-in-time snapshots, and hybrid recovery solutions."

Shiji Sujai



Evolution of DR solutions

DRaaS: KEY FEATURES AND BEST PRACTICES

HETEROGENEOUS PHYSICAL/VIRTUAL ENVIRONMENT SUPPORT

DRaaS solutions should be able to support a range of leading virtualization platforms—like VMware or Microsoft's Hyper-V—as well as physical server-based environments. Integration with existing technology capabilities like storage and hypervisor/VM-level replication is also important, because it helps organizations optimize their existing IT investments. Support for diverse platforms and replication options is a key indicator of a good DRaaS solution.

TESTING AND DOCUMENTATION

The versatility of a DRaaS solution lies in its ability to make the DR testing experience as smooth as possible. DR testing should be supported for different environments with minimal disruption to businesses. Frequent DR testing is recommended to verify the practicality of the BC/DR plans, and to avoid last-minute surprises. Previous DR test results should be accessible in the DR tool to fine tune the plan periodically—this also serves as documentation during BCDR compliance audits.

SERVICE MANAGEABILITY

While enabling end-to-end orchestration capabilities, service providers should also be able to provide customers granular control of defining DR parameters like RPOs, RTOs, SLAs, as well as resource specifications like processor and memory allocation. The solution should also provide a single management panel for failover and failback, irrespective of the recovery architecture, i.e. on-premises-to-on-premises, on-premises-to-cloud, or cloud-to-cloud.

"A good DRaaS solution supports a range of leading virtualization platforms and is frequently tested to support the most minimal disruptions to business continuity."

SOLUTION RESILIENCY

The underlying cloud storage layer in leading DRaaS solutions often has built-in resiliency. If the primary cloud storage device becomes unavailable for any reason, the backup VM images and data should be available from a different region. This resiliency should be backed by well-defined SLAs and support plans.

SECURITY AND COMPLIANCE STANDARDS

The DRaaS solution provider should ensure data security at rest and in transit by adopting industry-standard encryption technologies. Other best practices like role-based access control, safe-data disposal, identity management, etc., should be factored in to provide a secure solution. Depending on the industry vertical, many leading organizations consider compliance with respective industry standards—such as SSAE 18 SOC 2, DoD 5220.22-M, NIST 800-88, ITAR, FISMA, HIPAA and PCI—as key differentiators when selecting a DRaaS service provider.

ADDITIONAL VALUE PROPOSITION

Selecting service providers that can accommodate industry-specific requirements for sectors such as healthcare, government, financial, and banking may be an important consideration based on an organization's requirements. Moreover, the ability to cater to specific hardware requirements,

hybrid environment integration, and the availability of seasoned technical support and professional services teams could be decisive factors when choosing DRaaS service providers.

CUSTOMER EXPERIENCE

In addition to a myriad of technical capabilities, features, and best practices, the importance of a positive customer experience should not be underestimated. DRaaS service providers that prioritize customer experience often succeed in building a strong and loyal customer base.

CLOUD-BASED DR MARKET ANALYSIS

Let's look at the pros and cons of different replication and recovery orchestration tools that underpin DRaaS-based solutions of leading vendors.

VMWARE

vCloud Availability for vCloud Director (vCAv) provides replication of on-premise vSphere VMs to vCloud Director cloud environments.

01 VMware

Pros

- Self-service DR option for VMware virtual machines
- Support for DR failover, failback, and planned migration of workloads
- Flexibility to adjust compute and storage requirements in accordance with DR requirements
- Offline data transfer to support DR of large environments
- Availability of private, leased-line network features for replicating data between on-premises data centers and vCloud Air

Cons

- Limited to VMware; lacks support for heterogeneous environments (e.g. Hyper-V/Physical)
- Limitations on vSphere Replication depending on which customer needs to invest in advanced array-based replication technologies
- Lacks support for multiple public cloud environments as a target location
- Solution isn't affordable for some small- and medium-sized businesses

VEEAM

Veeam provides DR solutions for vSphere and Hyper-V virtual environments, without requiring the installation of any additional software.

02 Veeam

Pros

- Multi-hypervisor support can accommodate VMware and Hyper-V environments
- Hassle-free management with Veeam Availability Suite v9 console
- Granular, agentless data restores
- Supports self-service testing
- Affordable pricing for an enterprise solution
- Integration with deduplication tools that provide enhanced performance and efficiency

Cons

- Limited support for on-premises physical servers and applications
- Consumes more backup storage due to relatively low deduplication ratio
- Significant learning curve for administrators to select optimized protection options for certain workloads
- Requires additional infrastructure in the cloud for protecting cloud workloads, generating additional resource and license costs
- Veeam's Cloud Connect focuses on MSPs and does not provide API integration with public-cloud object-storage services

ZERTO

Zerto uses hypervisor-based replication technologies to simplify disaster recovery and to reduce storage costs.

03 Zerto

Pros

- Able to support RTOs as brief as a few seconds, enabling near real-time protection
- Heterogeneous platform support and architecture support for VMware, Hyper-V, on-premises-to-on-premises, and on-premises-to-cloud (AWS, Azure, IBM Cloud)
- Provides recovery points for up to 30 days prior
- Automation and orchestration of failover/failback, to deliver lower RTOs
- One-to-many simultaneous replication from primary site to DR site, and public cloud platforms

Cons

- Focuses on Hypervisor-level replication; lacks support for physical servers
- Additional infrastructure required in-cloud to enable DR
- Expensive licensing model
- DRaaS offering involves third-party channel partners, adding complexity to the solution
- Complex deployment architecture that requires management VMs per vCenter/SCVMM and Hypervisor

CARBONITE'S DOUBLETAKE

DoubleTake provides basic DraaS capabilities by replicating critical systems from the primary environment to the secondary target location.

04 Carbonite's DoubleTake

Pros

- Continuous replication provides always-on data protection
- Data recovery in minutes
- Optimizes resource utilization by leveraging encryption in-flight, compression, and bandwidth throttling
- Self-service testing without production disruption
- Historical snapshots that facilitate multiple recovery points

Cons

- Focused more on backup and high-availability space rather than a true DR solution
- Requires deployment of proprietary technology to all targeted systems
- Expensive licensing model
- Limited documentation causes steep learning curve for implementation and operations

AZURE SITE RECOVERY

Azure Site Recovery is a heterogeneous, workload-aware, and hybrid DRaaS offering, based on the Microsoft Azure cloud.

05 Azure Site Recovery

Pros

- Supports VMware, Hyper-V, and physical server recovery to the cloud, as well as to a secondary data center
- Availability of application-consistent snapshots for single or N-Tier applications
- Integration with SQL always-on, and other application-level replication technologies
- Able to create and test multi-tier application plans
- Supports planned, unplanned, and test failovers
- Integration with PowerShell and Azure Automation for end-to-end orchestration and failover of workloads

Cons

- Complex architecture for primary to secondary data center failover scenarios
- Only supports Azure as target for cloud failover
- Limited integration with other public cloud platforms. Supports only one-way migration to Azure from AWS. Failback is not supported
- Risk of vendor lock-in

This table summarizes the availability of the critical DRaaS features in each of the solutions discussed above.

	VMware	Veeam	Zerto	Carbonite's DoubleTake	Azure Site Recovery
Self-Service DR	✓	✓	✓	✓	✓
DR failover	✓	✓	✓	✓	✓
DR failback	✓	✓	✓	✗	✓
Planned migration	✓	✓	✓	✓	✓
Offline data transfer	✓	✗	✗	✗	✗
Multi-cloud support	✗	✓	✓	✓	✓
Multi-Hypervisor support	✗	✓	✓	✓	✓
Storage optimization	✗	✗	✗	✗	✓
Simplicity of implementation	✗	✗	✗	✗	✗

SUMMARY

Choosing the right DRaaS solution depends on factors like supported workloads, application dependencies, virtualization technologies, required RPOs and RTOs, and budget. When implementing the solution, it is also important to follow industry-standard best practices.

In this study, we reviewed the main advantages of DRaaS solutions, and how they help address several acute business continuity challenges. Each different DR solution and DRaaS solution provider has its own benefits and drawbacks that should be taken into consideration when selecting a service provider. It is also possible that a combination of solutions should be used.

As a managed-cloud service provider, Navisite provides services that enable organizations to implement a data protection and replication program, or implement a full disaster recovery as a service (DraaS) program that supports business continuity and meets business and compliance requirements. To learn more, visit our website.

ABOUT NAVISITE

Navisite, LLC, a part of Spectrum Enterprise, is a leading international provider of managed cloud services, including managed multi-cloud Infrastructure as a Service (IaaS), Managed Office 365 and Managed Applications. Navisite provides a full suite of dependable and scalable managed services, enabling enterprises to extend their data centers with hybrid, private and multiple public clouds. Enterprises can outsource IT infrastructure to Navisite to maximize the agility and value of their IT investments. With more than 1100 certifications held by Navisite employees, clients depend on us for customized solutions, delivered through an international footprint of state-of-the-art data centers. For more information, visit Navisite.com or Navisite.co.uk.

ABOUT THE AUTHOR

Chris Patterson Chris manages Navisite's Data Protection product development. Prior to Navisite, Patterson spent nine years at MTM technologies as the Director of Information Security Services, developing and consulting on security policies to the financial, retail, legal, health care, and public sectors. He holds a Bachelor's of Science in nuclear engineering from Worcester Polytechnic Institute and currently lives in Delaware.
- Connect with Chris on Twitter at @CPattCloud

Spectrum ENTERPRISE | Navisite™