DISASTER RECOVERY | 101

WHY YOU NEED DR

eBOOK

1 | WHY YOU NEED DISASTER RECOVERY

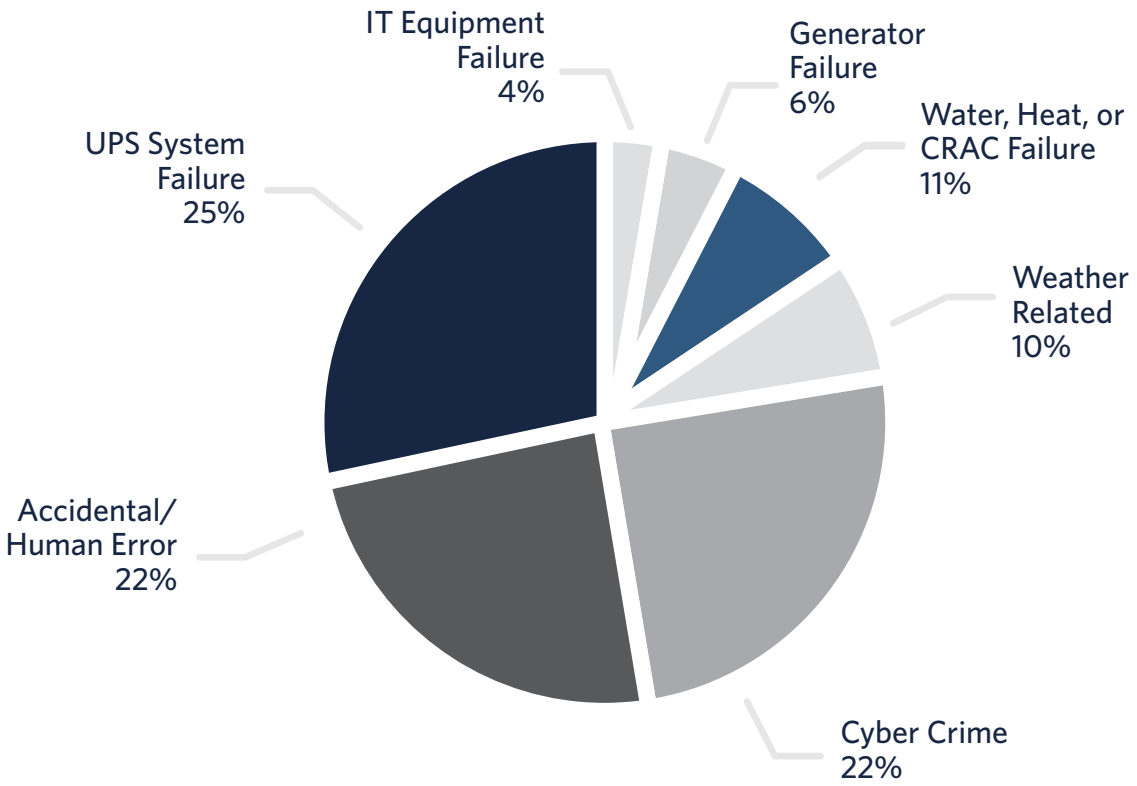
DISASTER RECOVERY 101

EVERYTHING YOU HAVE ALWAYS WANTED TO KNOW ABOUT DR – BUT WERE AFRAID TO ASK.

Confused about RTOs and RPOs? Fuzzy about failover and failback? Wondering about the advantages of continuous data protection over snapshots? Well, you are in the right place.

The Disaster Recovery 101 guide will help you learn about DR from the ground up and assist you in making informed decisions when implementing your DR strategy, enabling you to build a resilient IT infrastructure.

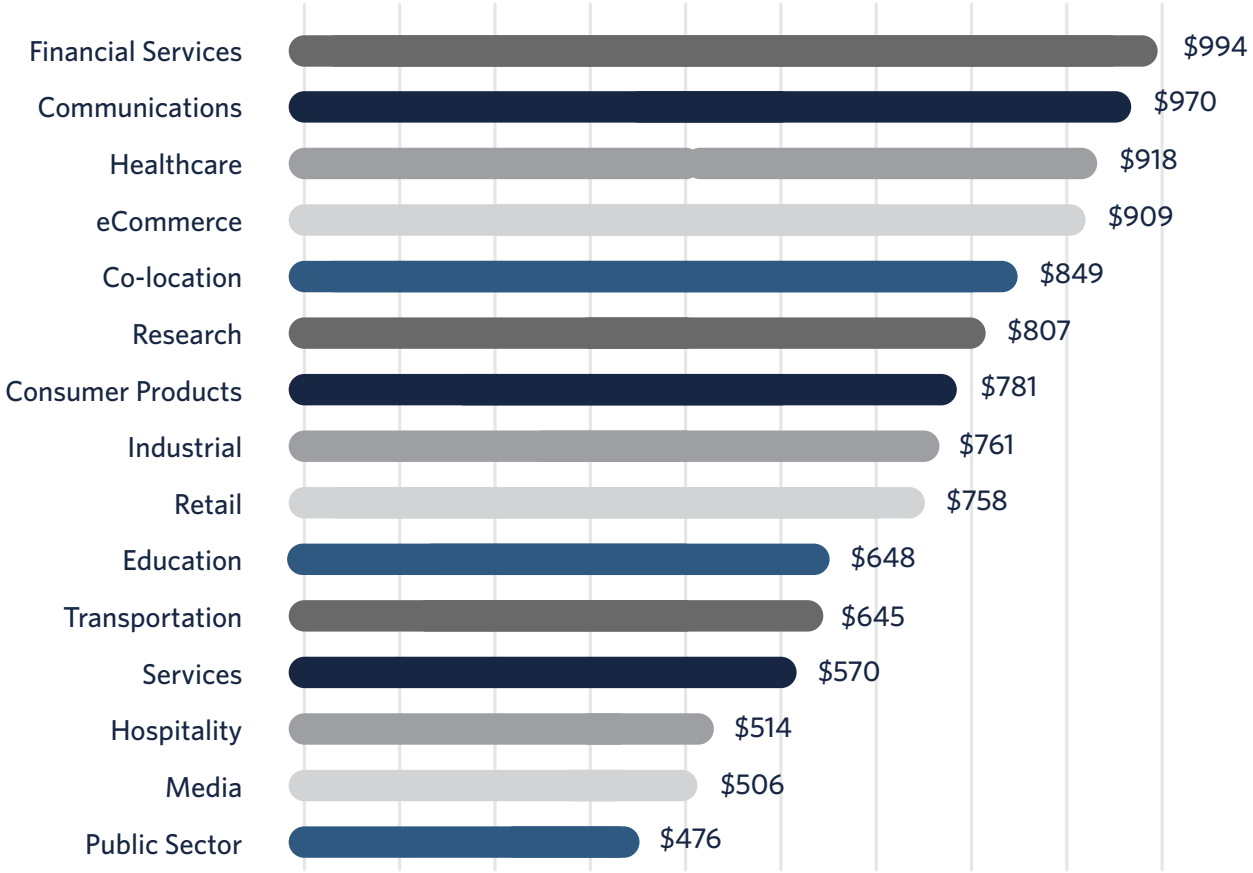
Root Causes of Unplanned Outages 2016



Source: Cost of Datacenter Outages- Ponemon Institute

NO ONE IS IMMUNE TO DOWNTIME

COST PER DATACENTER OUTAGE BY INDUSTRY



(Amounts shown in thousands)

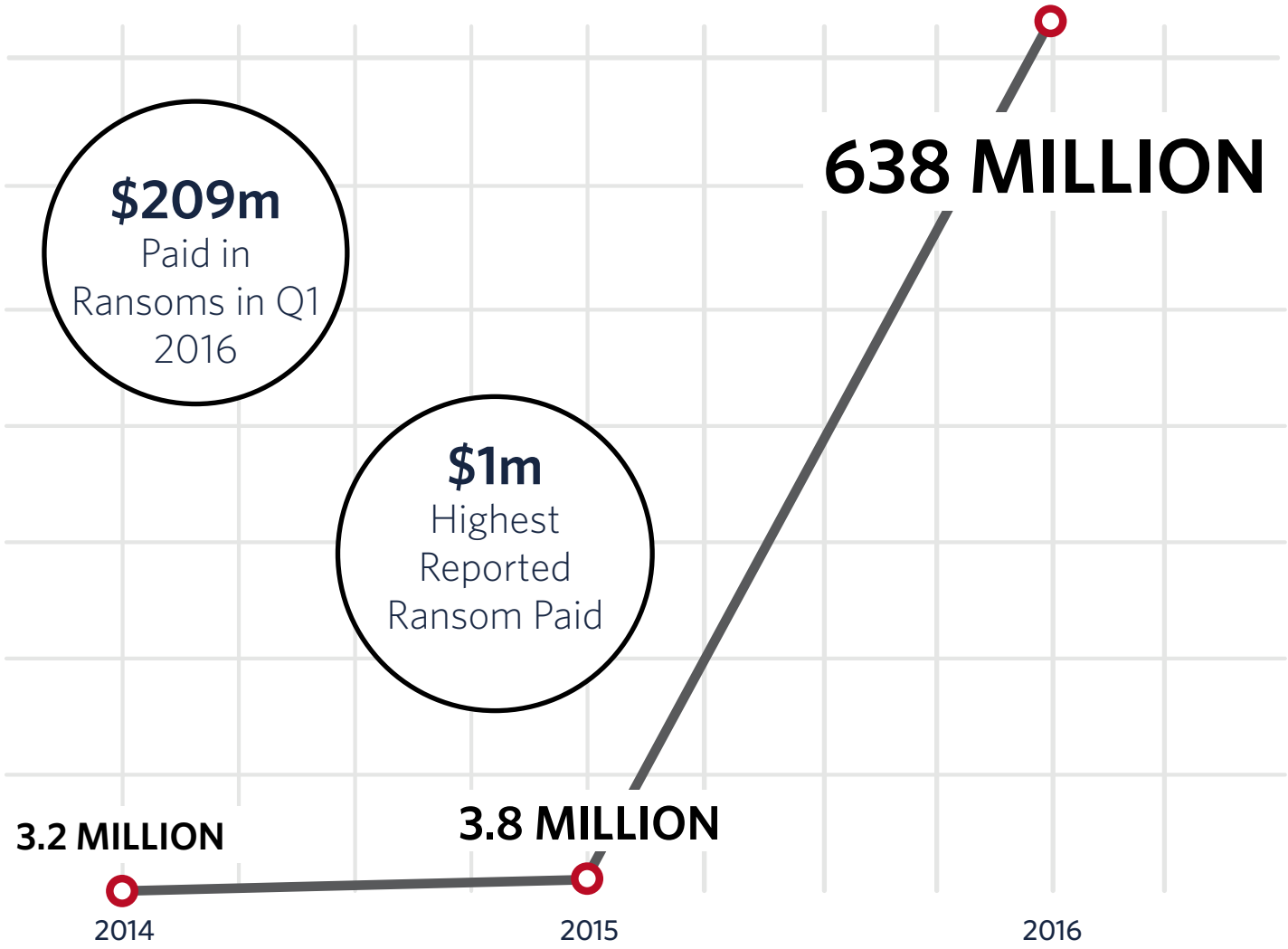
Modern businesses cannot afford to lose data. Whatever the cause – natural disaster, human error, or cyber-attack – data loss is costly and extremely risky to the life of a business.

The need for a business continuity strategy to ensure uptime, minimize data loss, and maximize productivity in the midst of any compromising situation is a necessary digital assurance policy for any company. The question becomes when will a disaster strike, not if it will.

Source: Cost of Datacenter Outages – Ponemon Institute

THE GROWING THREAT OF RANSOMWARE

NUMBER OF ATTEMPTED RANSOMWARE ATTACKS



Source: 2017 Sonicwall Annual Threat Report

2 | MEASURING DOWNTIME

MEASURING DOWNTIME

INTRODUCING RTO & RPO

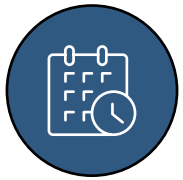
Recovery Point Objective (RPO) is the last point-in-time IT systems and applications can be recovered to. It indicates the amount of data that will be lost, measured in elapsed time

- The cost of **ONE HOUR** of lost data for any size business is a significant amount. Scaled upwards, this becomes an even larger impact.
- Due to the RPOs importance on data loss, it is recommended to agree on an acceptable, achievable RPO on a per-application basis.
- Always aim for the lowest RPO possible, then configure alerts to warn if you are in danger of the achieved RPO exceeding your defined SLA. Ensure that your solution enables the prioritization of individual applications as per your agreed SLAs, should the bandwidth for replication become constrained.

Recovery Time Objective (RTO) is the time that it takes to recover data and applications, meaning, how long will it be until business operations are back to normal after an outage or interruption.

- The cost of downtime associated with waiting for applications and data to be recovered (RTO) can result in significant loss in revenue and productivity.

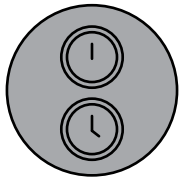
**Organization with a turnover of $100M*



DAILY BACK UPS

RPO - 24 Hours

UP TO $273,972.60*



SNAPSHOT-BASED REPLICATION

RPO - Hours

UP TO $45,662.10*

CONTINUOUS REPLICATION

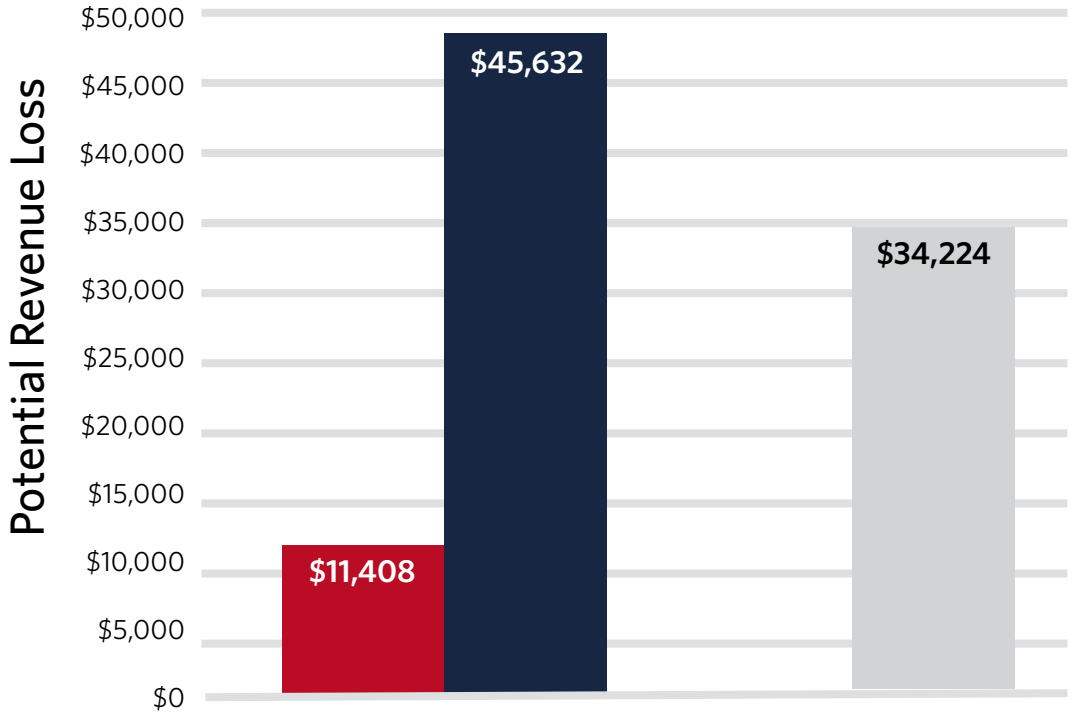
RPO - Seconds

UP TO $7,610.35*

WHAT DOES DOWNTIME COST YOU?

POTENTIAL REVENUE LOSS

For a company with annual revenues of $100M

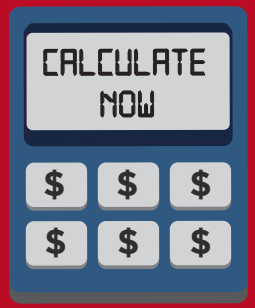


» The actual revenue loss can be significantly worse if the disaster occurs during working hours.

Downtime Calculator

WHAT WOULD DOWNTIME COST YOU?

It may be more than you think.



How much could downtime cost your organization?

Try our **Downtime Calculator**

Recovery Report for Virtual Protection Group Production 3

Report was generated on 09/14/2016 12:02:29

Recovery Operation Details

Initiated by	System	
Recovery operation	Failover Test	
Point-in-time	09/14/2016 11:46:17	
Recovery operation Start Time	09/14/2016	15:46:30
Recovery operation End Time	09/14/2016	16:01:07
RTO	00:07:43	
Recovery operation result	Passed by user	
User Notes	Stop Test for VPG Production 3	

Virtual Protection Group Recovery Settings

Protected Site	Production
Recovery Site	Culpeper Prod
Default recovery host	Prod 1
Default recovery datastore	DSXtremCP6
Journal datastore	DRJOURNAL01
Default test recovery network	Zerto_TestNet
Default recovery folder	DR

Detailed Recovery Steps

#	Step Description	Result	Start	End Time	Executi
1.	Fail-over test VM 'c3putdmo2212d1'	Success	11:46:32	11:46:42	00:00:09
1.1.	Create Recovery VM 'c3putdmo2212db1'- testing recovery'	Success	11:46:33	11:46:38	00:00:05
1.2.	Reconfigure IP for VM 'c3putdmo2212db1'- testing recovery'	Success	11:46:41	11:46:41	00:00:00
16.	Fail-over test VM 'c3putdcts1'	Success	11:46:42	11:46:50	00:00:08
16.1	Create Recovery VM 'c3putdcts1''- testing recovery'	Success	11:46:43	11:46:49	00:00:06
16.2	Reconfigure IP for VM 'c3putdcts1' testing recovery'	Success	11:46:50	11:46:50	00:00:00
19.	Fail-over test VM 'c3pitdga2122ap1'	Success	11:46:42	11:46:50	00:00:07
19.1	Create Recovery VM 'c3pitdga2122ap1- testing recovery'	Success	11:46:43	11:46:47	00:00:03
19.2	Reconfigure IP for VM 'c3pitdga2122ap1'- testing recovery'	Success	11:46:49	11:46:49	00:00:00
20.	Fail-over test CM 'c3pitdoh2004ap1'	Success	11:46:42	11:46:50	00:00:07
25.	Fail-over test VMs' 'c3putdmo2212db1' volumes	Success	11:47:19	11:48:06	00:00:46
25.1	Create scratch volume for VM 'c3putdmo2212db1'	Success	11:47:19	11:47:44	00:00:24
25.2	Detach volume VMs' 'c3putdmo2212db1-0:1:' from	Success	11:47:47	11:47:56	00:00:08
27.1	Attach volume VMs' 'c3putdmo2212db1-0:1:' to	Success	11:47:54	11:48:02	00:00:08

BE PREPARED: TEST YOUR DR PLAN

In order to benchmark your RTO and tweak your BC/DR plan to minimize downtime, testing is a must. By testing your plan with a BC/DR technology that allows for no downtime in production or break in the replication, you can perform a test during working hours. This ensure you are able to fully recover and you can run through the recovery operation multiple times to get your RTO as low as possible.

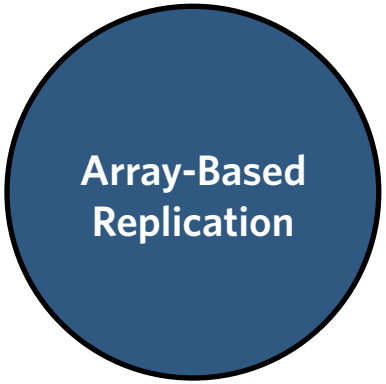
This is an actual successful failover test from a healthcare organization using Zerto Virtual Replication. The test was completed during a regular work day, with zero production impact.

This failover test covers the organization's tier one healthcare applications, consisting of 23 VMs with 8.3 TB of data, and took less than 15 min, with no downtime.

Note: Some data points in this report have been redacted to protect customer confidentiality.

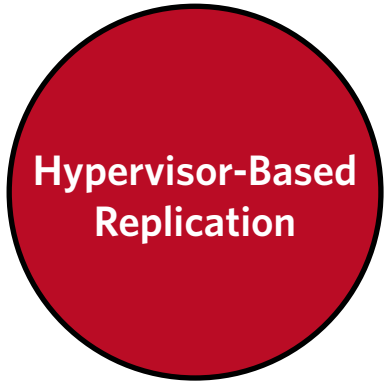
3 | COMPARING DIFFERENT REPLICATION TECHNOLOGIES

COMPARING DIFFERENT REPLICATION TECHNOLOGIES



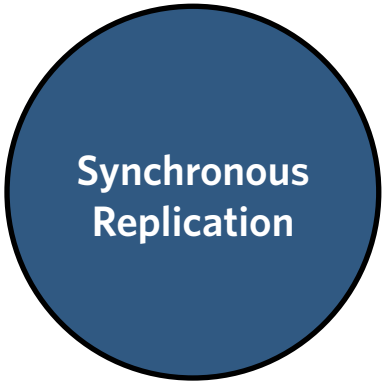
Sometimes called storage-based replication, these solutions are deployed as modules inside the storage array and replicate the entire LUN, regardless of its utilized capacity. They are designed for physical rather than virtual infrastructures and, as such, eliminate the benefits of virtualization.

Otherwise known as Guest-, or OS-based replication, these are software components that must be installed on each physical and virtual server. Although more portable than array-based solutions, the requirement to install modules on every server limits scalability.



As solutions designed to enable the full benefits of virtualization, these deploy a software module directly inside the virtual infrastructure. All writes are captured, cloned and sent to the recovery site at the hypervisor layer, making it more efficient, accurate and responsive than prior methods.

COMPARING DIFFERENT REPLICATION TECHNOLOGIES



Ensures all data is written in the source and target storage simultaneously, waiting for acknowledgment from both arrays before completing the operation. This relies on matching storage arrays and fiber channel latencies to minimize performance impact.

Uses snapshots to take a point-in-time copy of the data that has changed and sends it to the recovery site. The frequency is typically set on a schedule of hours, depending on the number and frequency of snapshots that the storage and application can withstand.

Near-Synchronous Replication is constantly replicating only the changed data to the recovery site within seconds— it's always on. It does not need to be scheduled, does not use snapshots, and writes to the source storage without having to wait for acknowledgment from the target storage.

	Synchronous	Asynchronous	Near Synchronous
Networking			
Replicate over any distance, avoiding regional disasters	–	✓	✓
Compressible replication traffic	–	✓	✓
Utilize cheaper IP links including VPNs	–	✓	✓
Data Loss & Recovery			
*Data loss (disk & in-memory data)	–	–	–
*Data loss on disk writes	✓	–	–
Seconds of data loss on disk writes	–	–	✓
Seconds of data loss of all data (disk & in-memory)*	–	–	✓
Data corruptions immediately written to target	✓	–	–
Point-in-time recovery to increments in seconds	–	–	✓
Performance & Snapshots			
Always-on protection with no scheduling overheads	✓	–	✓
No site link performance overhead on writes	–	✓	✓
Snapshots for point-in-time recovery	✓	✓	–
No performance impact of snapshots	–	–	✓
No storage overhead for snapshots	–	–	✓
Application consistency without snapshots	–	–	✓
Point-in-time recovery to increments in seconds	–	–	✓

WHICH TYPE OF REPLICATION IS RIGHT FOR **YOU**?

Synchronous, Asynchronous, or Near-Synchronous

Each data replication technology has different attributes, and depending on the requirements of your workloads and SLAs, you can use the replication method that best meets your requirements.

*Subject to the frequency on which the application can quiesce writes to disk without the overhead of utilizing snapshots.

4 | HOW DO REPLICATION TECHNOLOGIES STACK UP?

SNAPSHOTS

"The main problem with snapshots is not only the potential for performance impact, it is the lack of granularity of the points-in-time for recovery they offer."

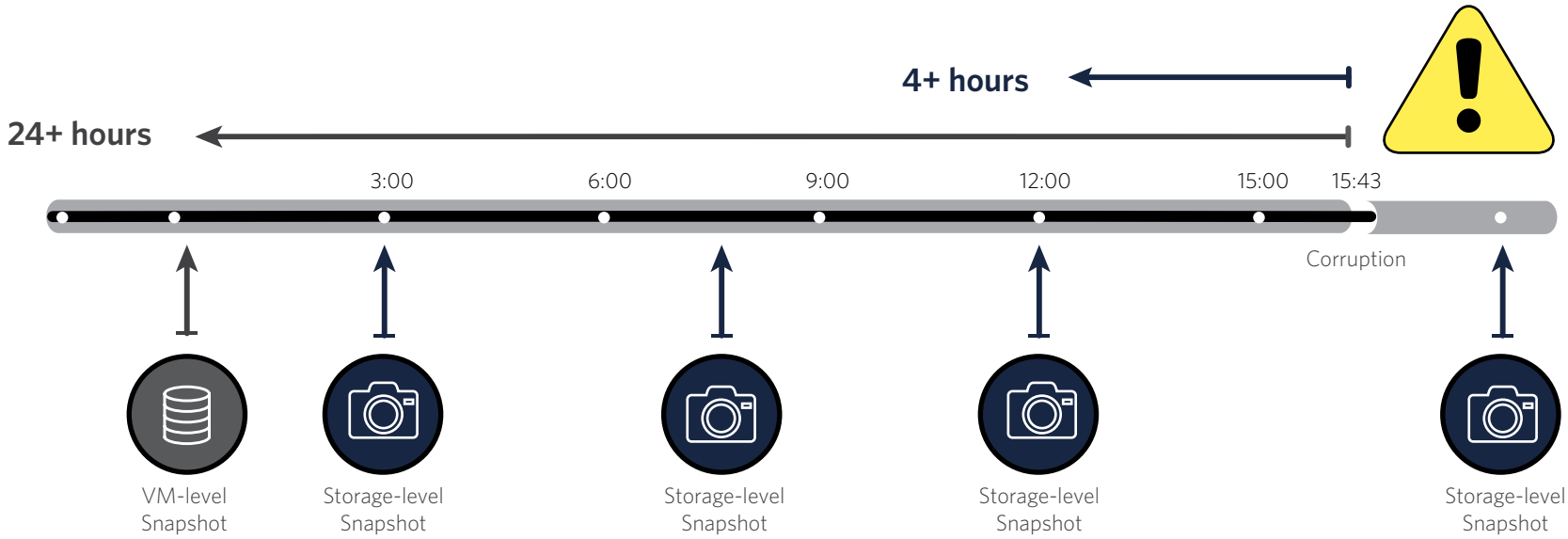
Virtualization Evangelist

VM-level Snapshots

VM-level snapshots are created in the hypervisor and incur the biggest performance impact. It is not recommended to create, remove or leave VM-level snapshots running on production VMs during working hours.

Storage-level Snapshots

Storage-level snapshots incur less performance impact than VM-level snapshots, but still require processing power in a storage controller, and at scale can still start to degrade performance. The potential for performance impact very much limits the frequency at which storage-level snapshots can be created.



If we take the above example of a data corruption at 15:43, then a VM-level 24-hour snapshot-based replication solution means you are going to potentially have nearly 16 hours of data loss, as you would have to restore a replicated snapshot from last night. The same example with storage-level snapshots would result in data loss of nearly 4 hours.

CONTINUOUS DATA PROTECTION (CDP)

"CDP will ensure our information is safe from any natural disasters or hacking incidents."

Bonyang Goo | Deputy Director IT Development Department | Seoul Daily News

Continuous Data Protection (CDP)

Continuous Data Protection (CDP) utilizes change-block tracking at the hypervisor layer to constantly replicate data as it is written to storage. Because CDP replicates only changed information, rather than an image of the entire host or array, there is no impact to the performance of the replicated VM.

Hypervisor-based CDP also utilizes journal technology to keep a log of all the changes occurring in a specified journal time frame, allowing point-in-time recovery in increments of just seconds for the length of the journal.

Because CDP is always on and always replicating the most recently changed data, it offers considerably lower RPOs than snapshot-based solutions. This results in significantly less data loss to the business and consequently, a far lower cost of impact.

Additionally, utilizing journal technology rather than VM-level snapshots for point-in-time recovery delivers multiple benefits beyond simply the sheer number of checkpoints available.

Replication Technology	RPO	RTO	Financial Impact
VM Level Snapshots	24 Hours	24 Hours	$821,917
Storage Snapshots	4 Hours	4 Hours	$136,986
Continuous Data Protection	20 Seconds	15 Minutes	$2,980

SNAPSHOTS vs CDP

SNAPSHOTS	CDP
Storing multiple snapshots on replica VMs incurs a significant VM performance penalty if you attempt to power on the replica VM.	With journal-based protection, the journal is only used until you commit to the point-in-time selected, without the performance impact of many snapshots.
Using snapshots on replicated VMs allows no way of controlling the total space used for snapshots, or the ability to store the data change on a separate datastore. This makes it unscalable in terms of being able to set SLAs and define maximum limits on the data space used by the snapshots.	With journal-based protection, you can place the journal on any datastore and place maximum size limits and warnings; so as not to fill the datastore, which could otherwise break replication and recovery.
With snapshot-based replication, there is often significant overhead on the storage arrays for replication reserves; which can be 20-30% on both source and target storage in many cases.	With journaling technology, no extra space is used in the source storage as no snapshots are created. Only 7-10% of the target storage is typically used for the changed data, freeing up significant amounts of disk space.

COMPARING BACKUP & REPLICATION

BOTTOM LINE

Backup is a relatively inexpensive way to avoid complete data loss. Valuable for compliance. Does not ensure continuity of operations.

Replication is focused on ensuring that business applications and processes are always available, even after a disaster. More expensive to set up and maintain.

HOW IT WORKS

Backup typically relies on snapshots which are copies of the data set taken at a pre-determined point-in-time.

Replication can be Synchronous, Asynchronous or Near-Synchronous and may use Continuous Data Protection to enable users to access historic data.

DEFINITION

Backup involves making a copy or copies of data.

Replication is the act of copying and then moving data between a company's sites. It is typically measured in Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

REQUIREMENTS

Backup requires a tape library (usually VTL doing disk-to-disk backup) and some place to store archived tapes.

Replication requires investment in another infrastructure in order to enable recovery and continued business operations.

USES

Backup is typically used for everything in the enterprise, from critical production servers to desktops.

Replication is often used for mission-critical applications that must always be up and running.

PURPOSE

Backup focuses on compliance and granular recovery, such as long-term archival of business records.

Replication and recovery focus on Disaster Recovery — quick and easy resumption of operations after a disaster or corruption. Minimizing the Recovery Time Objective (RTO) is key.

5 REASONS

WHY BACKUP IS NOT DISASTER RECOVERY

1 Service Levels

Backups typically happen once per day and at night, so your RPO could be 23 hours! When protecting mission-critical applications, 23-hour data loss is not acceptable. Without any recovery orchestration, the RTO will also be significantly higher. Rebuilding a virtual machine and everything that goes with it, from tape, can take days; from disk, it might be slightly faster — a few hours.

2 Application Impact

Backups occur at night because making a copy of an application and its data drains the CPU on the server. If you need more aggressive RPOs than 23 hours as stated above, that means you have to create copies more frequently. This is possible, but at the expense of CPU. This significantly impacts end-user productivity.

3 Automated Recovery

Building an environment from a backup, especially a tape backup, is extremely time consuming. This is why the RTOs are so long. With an enterprise-class disaster recovery solution, the entire recovery process can be automated. For mission-critical applications, this entire process should take just a few minutes. This is a very different service level from a backup solution. Additionally, an automated process is a foolproof process, since every manual step that is introduced is an opportunity for an error.

4 Retention

Backups are typically stored for a very long time for compliance and audit purposes. Disaster recovery information is stored for hours or days. Additionally, for a backup, you will have just one snapshot of the application and data. For an enterprise-class disaster recovery solution, you will have several points in time to failover to, just in case the last point-in-time is corrupted.

5 Reverse Replication

In the event of a disaster, once an application has been made available on a target site, you must extend that application's protection to include new data being created. However, you must make sure that this application continues to be protected as the users create additional data. A backup solution will not start taking backups and ship them back to the production site. A disaster recovery solution will ensure the application is still protected by replicating back to the source site.

5 WHY RECOVERY AUTOMATION & ORCHESTRATION IS IMPORTANT

MANUAL RECOVERY, SCRIPTED RECOVERY, AUTOMATION & ORCHESTRATION SOFTWARE

Manual & Scripted Recovery

Many organizations choose manual or scripted recoveries due to the cost and complexity of buying and installing a solution just to handle the recovery and testing operations. Testing frequency is also impacted as downtime is required to conduct the tests, which in combination with staffing overheads introduces a significant risk of the business not being able to recover from a disaster.

This means that most synchronous replication based environments have RTOs measured in hours to days, as the recovery needs to be performed manually or by using untested scripts. The extended disruption to business operations caused by the long recovery process can have a significant financial impact.

Some synchronous replication solutions are used as part of a metro-cluster, High Availability (HA) solution. In this configuration, all the VMs are randomly restarted in the secondary datacenter by a HA service in the event of power loss. This scenario results in a potential RTO of many hours, as the VMs are not recovered consistently or in the correct order, requiring manual reconfiguration by multiple administrators in order to restore operations.

Automation & Orchestration Software

Hypervisor-based replication includes replication, recovery automation and orchestration all-in-one solution. The VMs that form each application are recovered together in consistency groups from the same point-in-time. Boot-ordering is then applied to ensure that the VMs come online in the correct order, and re-IP or MAC addressing can be utilized if needed to ensure there is no break in communication. This ensures an RTO of just minutes with no manual operations required as the application is automatically recovered in a working and consistent state.

No-impact failover testing also enables this automated process to be tested during working hours in minutes, with no shutdown in production or break in replication. Reports can be generated to show the testing outcomes and prove the recovery capability. This enables organizations to increase the frequency of DR testing, mitigate risk, and satisfy compliance initiatives.

6 TOTAL COST OF OWNERSHIP CONSIDERATIONS (TCO)

TCO OF TRADITIONAL ARRAY-BASED REPLICATION VS. HYPERVISOR-BASED REPLICATION

MAIN CONSIDERATIONS TO REDUCE YOUR TCO

Snapshot Space Utilization & Cost

Challenge: Snapshot solutions typically consume more than 20% of both the source and target storage, plus an additional 5% of replication reserve space. The cost and overheads of utilizing array-based replication must therefore include the cost per GB/TB multiplied by the storage usage of the snapshots and replication reservations.

Solution: The ability to recover to previous points in time is enabled by keeping a journal on the recovery site storage, which dynamically grows and shrinks to the size of the changes in time it is configured to keep.

Recovery Orchestration & Automation

Challenge: Utilizing storage replication simply creates a copy of the data in the recovery site. To recover the data during testing or a DR event, it needs to either be done manually using scripts, or by utilizing an orchestration and automation solution. Due to the time it takes to recover manually and the difficulty in conducting tests, an additional orchestration and automation solution is recommended. The cost of purchasing the licensing of the additional solution and managing multiple solutions should therefore be factored in.

Solution: Hypervisor-based solutions include recovery automation and orchestration features such as application-consistent VM boot-ordering, re-IP/MAC addressing and custom pre-/post-scripting, in addition to the continuous replication technology. This significantly reduces the RTO as well as the cost and complexity of managing multiple solutions.

Storage Lock-In

Challenge: Array-based replication solutions are vendor-specific and require matching storage arrays in both the source and target sites. This can significantly increase the TCO of the next storage refresh by having to buy new and matching storage arrays, just to configure replication. There is no ability to mix storage vendors and technologies to get the best price-to-performance ratio in a recovery site, or to introduce new storage vendors to improve performance.

Solution: Hypervisor-based replication operates at the virtual, not physical layer, meaning it is inherently storage-agnostic. This allows you to buy or use any storage in any site, reducing the TCO of your next storage refresh and enabling the seamless adoption of new technology. Even if the same storage is used in both source and target sites, replicating from the hypervisor removes complexity to save on the cost of management overheads.

7 NECESSARY ELEMENTS FOR A SUCCESSFUL DISASTER RECOVERY PLAN

Your disaster recovery plan consists of more than just how you are going to recover your systems and applications. When a disaster happens, there is a lot involved before recovery is initiated.

7 ELEMENTS

1. COMMUNICATION

Ensure lines of communication between employees remain open during a disaster. Services you normally rely on might be limited or unavailable. Don't depend on email or cell phones. Make sure landline numbers are accessible and even think about two-way radios. Consider arranging a certain location where people can meet, if all else fails.

2. CONTACTS (ROLES & RESPONSIBILITIES)

Who does what? The roles and responsibilities of everyone involved in the DR plan should be clearly laid out. Individuals should be aware of their specific duties and everyone needs to know whom to contact to get the ball rolling. Ideally, you should have a backup assigned for each role, but certainly for those key decision makers.

3. LOGINS

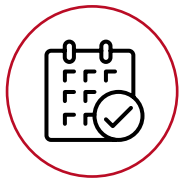
Hopefully, the only person with access to initiate your recovery process is not on holiday, trekking in the mountains without a phone signal. Restricting access to only the people who need it is certainly a good idea, but make sure there is more than one person who can access the systems necessary to perform the recovery.

4. REMOTE ACCESS TO INITIATE RECOVERY

We are rarely tied to a single location during our daily routines, so the ability to monitor and manage operations remotely becomes of great benefit. In a disaster situation, however, you may not have access to your primary facility at all. Ensuring that you are able to initiate your disaster recovery plan from another remote location is vital.

5. DOCUMENT EVERYTHING

Absolutely every essential activity that makes up your disaster recovery procedure should be written up with clear instructions and directions. This includes the areas already discussed but should also include step-by-step guides for people to follow. Having processes clearly described can help maintain calm and control.



6. TEST YOUR PLAN, THEN TEST IT AGAIN!

Testing the failover capabilities of your disaster recovery solution is of crucial importance to make sure it works when needed. But it is just as important to test the rest of your plan and make sure it is just as robust. Test at least once a year – preferably more – and make sure the team is as familiar as they can be with their duties.

7. UPDATE YOUR PLAN

A final, small and maybe obvious point, but a very important one: Make sure your plan is up-to-date. If it's 5 years old, you are asking for trouble. Please... update, update, update!

8 | THE FUTURE OF DISASTER RECOVERY

DISASTER-RECOVERY-AS-A-SERVICE

(DRaaS)

Since a dedicated DR site can be expensive to maintain and scale, many organizations are looking to outsource the costs. Replacing the costs of a secondary site (hardware, software, power, cooling, maintenance, etc.) with a predictable monthly expense is a very attractive option. DRaaS has become increasingly popular as a way for organizations to reduce the time, resources, and costs of hosting and managing their own DR solution.

DRAAS OPTIONS

1

Managed Service

A fully managed service, where all of the secondary site infrastructure is provided at a rental cost and the tasks of managing and invoking the replication and recovery process are controlled by the service provider. For organizations that are not familiar or confident with implementing or managing a DR solution — or simply don't have the resources to do so— this can be a very useful option.

2

DIY Service

Alternatively, a hosted DIY service may be selected, in which case the secondary site infrastructure will be provided as before, but the process of managing the disaster recovery solution will be controlled by the customer. For those happy with taking on this responsibility, a DIY service can be a cheaper option than a managed one.

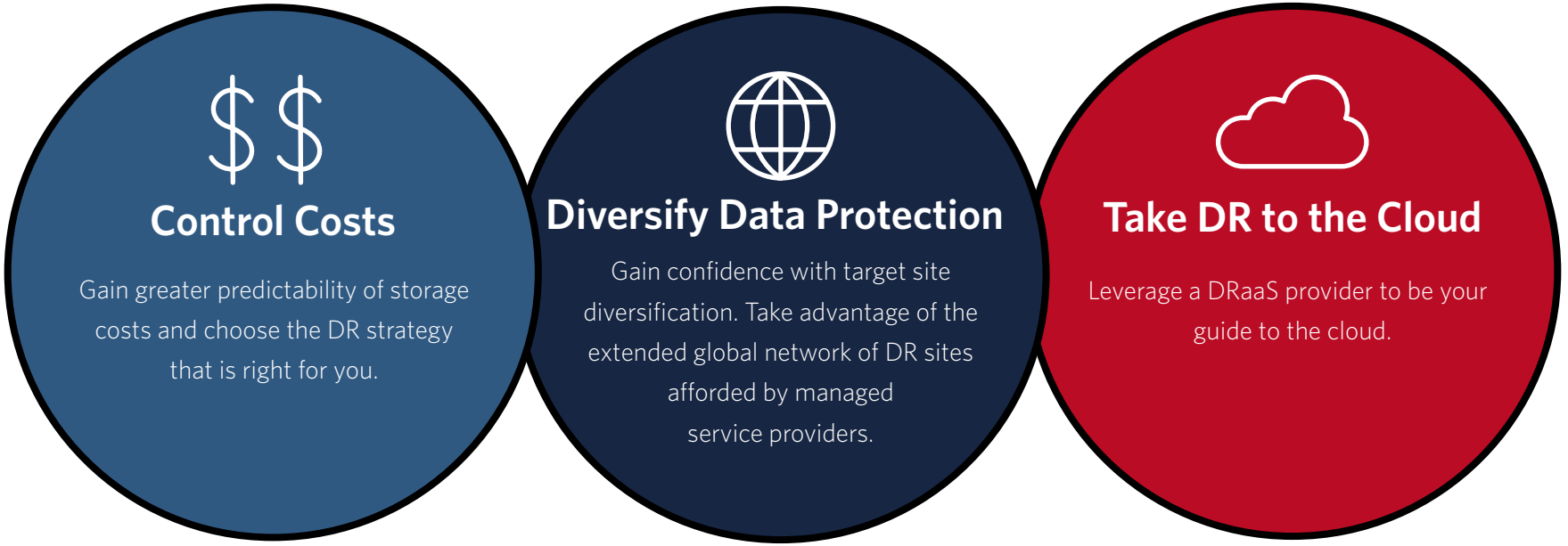
!

IMPORTANT TO REMEMBER

The type of disaster recovery solution used to protect your data will be dependent on the service offered by the provider. Ensure you know what solution you will be getting in order to fully evaluate the service and potential benefits.

WHY CONSIDER DRaaS?

DRaaS providers do this every day, so they are knowledgeable about getting environments online quickly and can help you avoid common mistakes. They also serve as additional resources that are focused on your datacenter recovery when you need it most.



HYBRID CLOUD/ PUBLIC CLOUD

Hybrid Cloud is rapidly becoming the preferred model for IT as it enables businesses to optimize their IT environment and gives them limitless choices. With a cloud based solution, all elements of disaster recovery can be structured based on target costs and SLA.

Disaster recovery, with its unpredictable bursting nature, is one of the best-suited processes to have in the public cloud.

Performance & Capacity On-Demand

Pay-for-what-you-use

Remove Second Site

Legacy DR solutions can however create many barriers to adopting a hybrid cloud strategy:

Different hypervisors and APIs create infrastructure silos, making it very difficult to leverage different clouds for the same workloads.

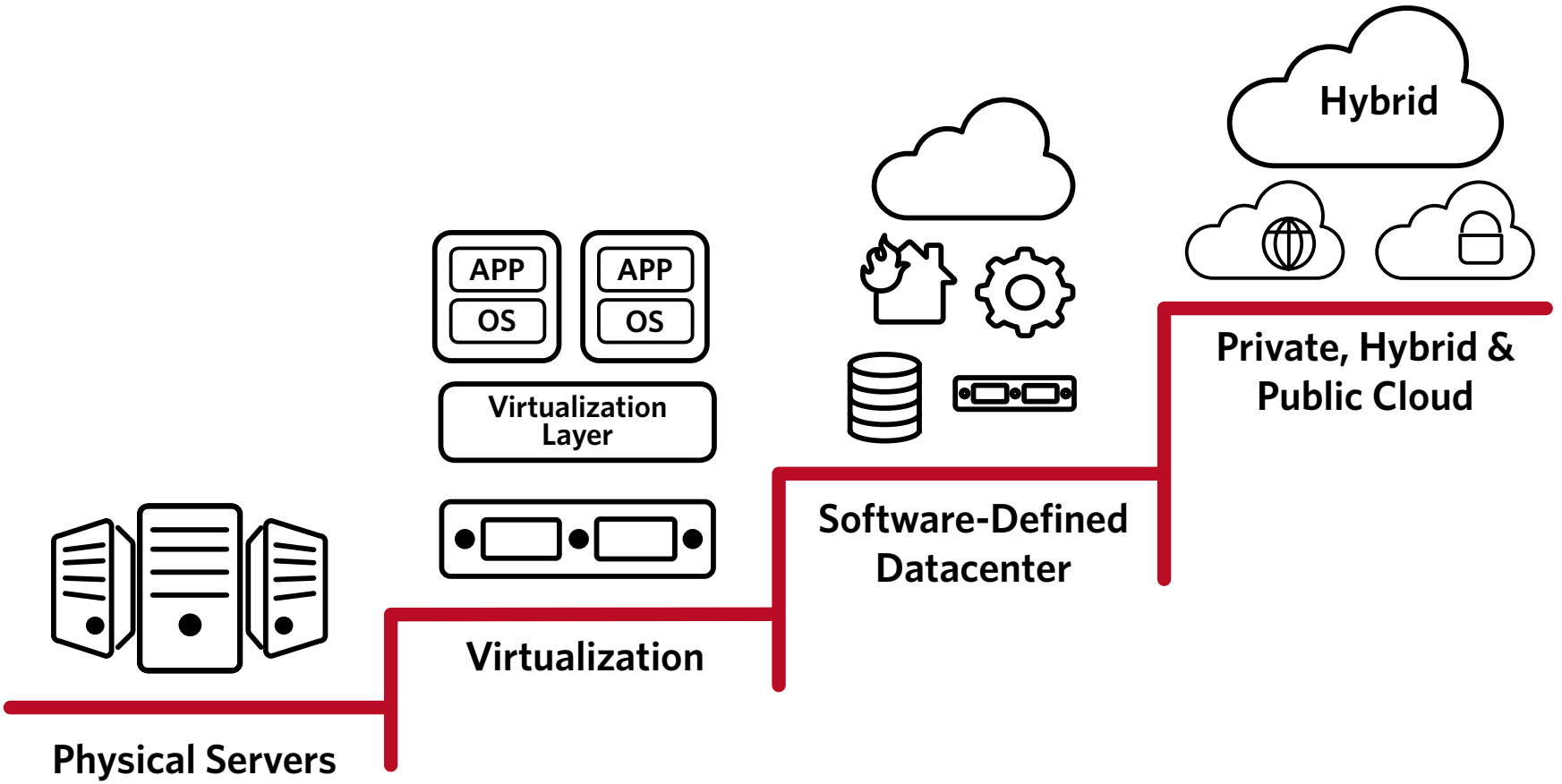
Applications cannot be easily replicated, managed, or used between different environments.

The initial reconfiguration and downtime costs associated with "bursting" into an environment, or replicating to a different silo are simply too high.

Having the right replication & recovery solution in place can overcome all these barriers, as it should not only serve as a protection solution, but also as a mobility solution. With the right solution, enabling disaster recovery in the cloud now can provide a stepping-stone to the future adoption of other, more critical services, as organizations grow more confident in the use and performance of the public cloud.

THE EVOLVING IT LANDSCAPE

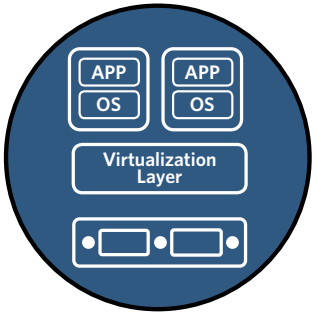
The landscape of modern technology is changing at a rapid pace, an example of this are the demonstrable changes in server technologies in recent history; evolving from physical hardware to cloud and beyond. The term IT resilience is a relatively new concept; born from the need for companies to continuously adopt newer and more scalable disaster recovery technologies. IT has evolved substantially, from the creation and evolution of virtualization, the software-defined datacenter and now the hybrid cloud. The need to maintain a robust infrastructure that remains flexible enough to withstand constant transformation has become essential, but continues to pose a difficulty for many organizations.



DIGITAL TRANSFORMATION

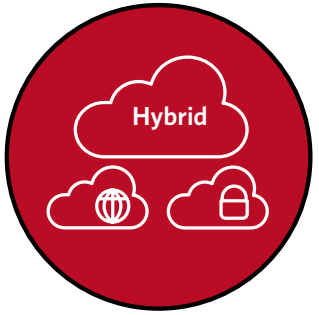
Digital Transformation describes the ongoing and everlasting process of upgrading and refreshing an organization's IT infrastructure. Ensuring the business stays up-to-date with modern developments and remains competitive is paramount, but becomes increasingly difficult as technology develops faster.

EXAMPLES OF TRANSFORMATION PROJECTS



Adopting a new hypervisor to support virtualization strategies

Implementing new software-defined methods of performing tasks previously requiring hardware investment



Embracing a private, hybrid, or public cloud strategy to remove a physical footprint altogether

Each of these processes will have unique barriers to adoption as you would expect, but by embracing the concept of IT Resilience organizations can significantly reduce, or even completely remove any barriers to success.

"With IT Resilience, organizations can withstand any disaster, confidently embrace change and focus on business."

24/7 BUSINESS

IT RESILIENCE

3 STEPS TO IT RESILIENCE

72%

Of companies have experienced an IT outage in the last year[1]

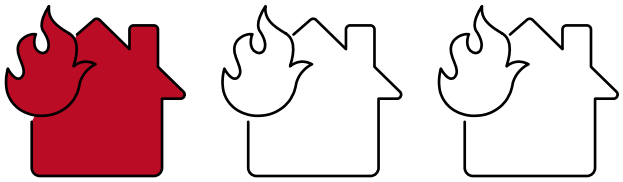
70%

Of enterprises that will have a hyprid cloud strategy by 2019[2]

- **Minimize Service Disruption**
- **Ensure Application Mobility**
- **Create Infrastructure Flexibility**

1 in 3

firms has had at least one declared disaster or major disruption during the past 5 years

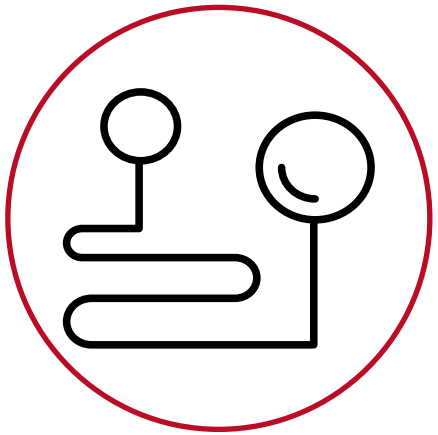


IT Resilience

IT Resilience has come about as a result of the long-overdue evolution of disaster recovery solutions to bring them in line with today's modern, virtualized infrastructure. By its very nature, the concept supports and enables the process of digital transformation by removing physical dependencies and enabling software-defined flexibility and data mobility.

It also provides truly enterprise-level protection of mission-critical data and applications, to provide organizations with the confidence to adopt these changes and simultaneously withstand any potential disruption to the business—be it a power failure, cyber-attack, or natural disaster.

Sources:
[1] Gartner BCM survey (https://www.gartner.com/doc/3200321/survey-analysis--bcm-survey)
[2] Gartner "The future of the Datacenter in the Cloud Era" (https://www.gartner.com/document/3079122?ref=unauthreader&srcId=1-3478922254)



CONCLUSION

SO, WHERE DO YOU GO FROM HERE?

In today's always-connected world, businesses need to be available to their customers, 24/7/365. Zerto provides Resilience for Evolving IT™, ensuring enterprises and their customers always have access to business-critical data and applications without any IT interruption, downtime, or delay. Our award-winning Cloud Continuity Platform™ is the simplest, most reliable BC/DR software solution built to protect applications on any virtualized IT environment, be it public, private or hybrid cloud. Zerto's proactive approach to recovery gives companies confidence in their ability to withstand any disruption, easily incorporate new technology, and quickly adapt to accommodate evolving IT priorities— all to move you closer to embrace IT resilience. Learn more at www.zerto.com.