Disaster Recovery:

Make the Case to Add It to Your IT Budget.

iland | VEEAM CSPPARTNER Platinum | cpp Infrastructure. Anywhere.

Contents

Business leaders across the globe may think disaster recovery (DR) is too expensive, too complex, or that a disaster is unlikely to impact them. Yet human error, cybercrime, or a natural disaster can cause their company's digital infrastructure to come crashing down in a split second. Then what?

The Reality of DR

Every year, IT teams are challenged to do more with less. The number of projects, advances and business requirements for IT grows, and it is a struggle to fit it all into the budget. One line item that is often cut is disaster recovery. People tend to think "Disasters happen to someone else. We'll get around to it next budget cycle." The reality is that DR is not a luxury, it's a necessity. IT has become a fundamental piece of every business and it is critical to be always available for your internal and external users.

When people think about disasters, they initially think of major natural disasters, such as hurricanes or flooding. But, most disasters come from less extreme but potentially more damaging factors such as:

Hardware faults

Every piece of hardware is rated for five nines of availability, but what happens if something fails? How does that impact what is running on it? What if there is data corruption because of it, or hardware replacement is more than four hours away?

Software faults

Let's be honest, no software package is perfect. Between integration into multiple systems, patches, vulnerabilities and common errors, what happens if your primary application has an issue that potentially loses data or fails to start?

Malicious software

You can't read the news without hearing the latest security vulnerability or worse, a ransomware or cryptolocker scare. If your organization's data is held hostage, how will you recover?

Malicious users

You hope that no one would ever intentionally do something to compromise customer or employee data, but it happens. With no recovery options in place this can be a burden on IT to resolve quickly, while also dealing with the human aspect of the disaster.

Accidents

Sometimes, someone just makes a mistake. It happens to everyone. Some mistakes are minor and can be solved easily, while others are more pressing and require immediate IT intervention.

"Although there's no magic answer on how much impact downtime will have on your business, current industry surveys have shown that the average enterprise estimates an impact of approximately $5,600 for every minute of unplanned downtime in its primary computing environment..."

–Gartner, "Three Moves for CIOs to Lower Business Costs with Clouds,"
Ron Blair, 24 March 2017

IT Resiliency

Every organization has backups, and many feel that is all they need to protect their environment. When looking at budget items, DR becomes an insurance item for something that hasn't happened so far and companies decided to pass and roll the dice. Backups are necessary for multiple reasons—long-term retention, file recovery and even system recovery. But backups are not disaster recovery. For a complete, fully resilient business continuity solution, organizations must employ both backups and DR.

"...DR becomes an insurance item for something that hasn't happened so far and companies decided to pass..."

Recovery Point Objective (RPO) is how far back in time you will go when recovering data in an event. Backups are traditionally run once a day at off hours, and thus can lead to unacceptable RPO timeframes. Imagine that a nightly backup is all that you have and something happens an hour or two before the next backup can occur. This potentially puts your organization back 20+ hours. How much data was lost? How many orders? How many projects? What is the impact of having to find and recreate 20+ hours of data?

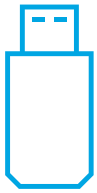
Recovery Time Objective (RTO) is how long it takes you to recover that information. Large data sets or even full systems can take hours to recover. When combined with an old dataset, your business could be down for over 24 hours from the recovery process time and the last known good state of your data. These numbers might be fine for certain tiers of workloads but every application and process needs to be evaluated. If it is mission-critical to your organization, and you can't afford for it to be down for 24 hours, it needs to be protected with disaster recovery techniques that meet the appropriate RPO and RTO.

While backups are necessary for organizations, there are other limitations to think about when relying only on them for data resiliency. Local backups can be impacted by either hardware faults or malicious software. Backup to disk is a great technique because of how rapidly you can recover data versus other, slower longer-term solutions. But, if there is a cryptolocker attack on that data or a hardware fault on the storage, you will effectively lose that and need to rely on your other copies of data that might be on slower devices or off-site. Another challenge is that backups need something to recover to. While natural disasters don't cause the most IT disaster incidents, they still do occur. Data center flooding, power outages or complete hardware failures mean there is nothing physically available to restore to. So, now you have your data, but nowhere to put it.

Business continuity and data resiliency rely on having overlapping coverages of protection based on the criticality of the application and system. Multiple backups leveraging the 3-2-1 rule of 3 copies of data, 2 different media types and 1 off-site is not only a good starting point, it's a must. But, add to that faster RPO/RTO options for disaster recovery based on the tier of system and you can start to build multiple protection schemes to limit the impact that a disaster can have on you.

3-2-1 Rule

3 copies of data

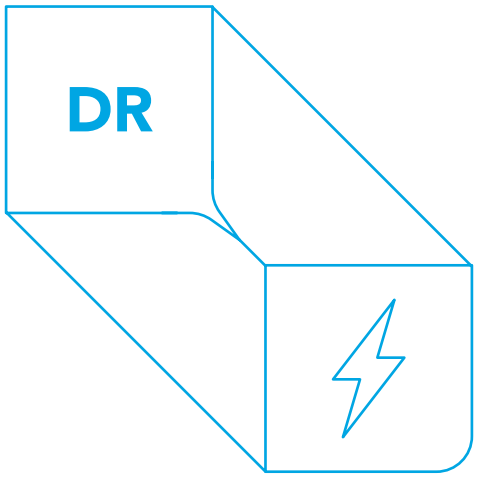


2 different media types

1 off site

Cloud Makes DR Affordable

Historically, one of the biggest hindrances to creating a DR solution was the enormous capital expenditure cost. This was usually seen in the budget and immediately cut out for being too expensive. Finding a secondary site or co-location, buying double the IT infrastructure gear, power, software and maintenance doubled an IT project's cost and DR became the first thing that was cut. The cost in man hours to configure, test and maintain a full second site just for disasters made the cost astronomical. As virtualization modernized the data center, it had huge benefits in disaster recovery. Now, you can protect your environment practically anywhere.



Cloud brings affordability, scalability and agility to disaster recovery. Cloud cost models are different than traditional CAPEX for IT. Instead of buying duplicate hardware, with maintenance and all of the associated secondary site costs, you simply pay for the storage you need, and in the case of a disaster, pay only for the resources you consume. This keeps cost a fraction of what building a secondary site would be, and allows you to always know what your bill will be.

Another significant benefit to cloud Disaster Recovery as a Service (DRaaS) is in the ability to tier your workloads for the proper RPO/RTO and manage costs based on that. If you are building a secondary site, you still need to purchase everything up front whether it's your tier 0 mission-critical app, or those development servers that get used once a month. With a cloud consumption model, you can decide what gets protected, how often and how or if it's brought online in the case of a disaster.

"Cloud brings affordability, scalability, and agility to disaster recovery."

Planning, implementing, testing, orchestrating and invoking a disaster recovery plan can be a huge ordeal for any IT team. Cloud technologies allow IT staff to quickly plan and implement a disaster recovery strategy that doesn't take months. Testing can be done non-intrusively and a majority of the time it is automated with full reporting. So, instead of traditional DR tests taking a full weekend and the entire staff's time, it can be run with a simple automation script on a Tuesday afternoon and verified the next day. If there are any issues, those can be addressed and the tests can be run again. This aspect can help give you complete confidence in your solution's viability if the need arises. All of this is done side by side with disaster recovery experts who can help you at any moment. When thinking about the cost and justifying DR, the ability to add a qualified DR staff to the line item for next to nothing becomes another appealing factor of cloud-based DRaaS.

While many disasters are unplanned events, there are occasions where you know that you could potentially be without power. Should a situation like that arise, DRaaS customers can fail over their environment into the cloud pre-emptively with little interruption and continue doing daily business while they focus on resolving the issue that caused them to failover.

Do More With DR

As you begin to justify the cost of DR and why it should remain in the budget, there are other things to consider that will further extend the value of a cloud-based DRaaS solution. Newer technologies that allow for seamless testing without impact give your IT team true flexibility beyond just simply testing. Because a DR test is an identical copy that is brought online in the cloud and isolated from your production environment, you can use that copy to perform many of the intrusive, out-of-band testing that was previously impossible. This feature to make a copy also has the benefit of not impacting the actual data replication, so your tests can be run with the knowledge that in case of a true disaster, you will still achieve the RPO goals set without any interruption. You can also run vulnerability scans or other data intensive file analysis scans and use those reports to remediate the production environment. When it comes to patch management or new software rollout, being able to fully test your upgrade on an identical copy of your production environment without impacting actual production is a huge boost to a successful upgrade or deployment. If there are any problems, they can be addressed in the cloud copy before the actual roll out. Environments can even be spun up for testing and user feedback.

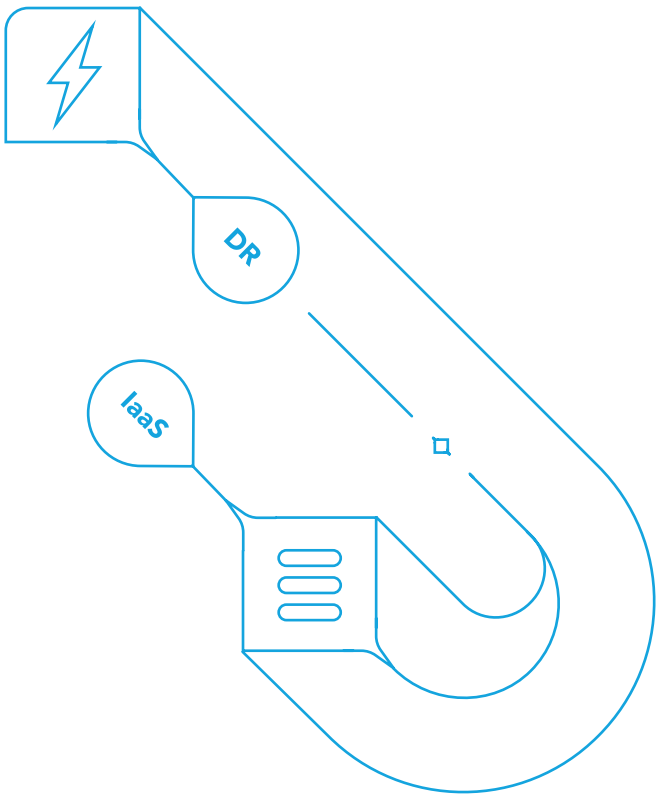
All of these capabilities and features are baked into your cloud, but not readily apparent when just looking at the total cost.

You Cannot Afford to Cut DR From the Budget

When you look at all of the things that an IT team needs to function, from software and hardware to infrastructure and people, it becomes very easy to redline the money you want to put into a new disaster recovery solution and think "maybe next year." You cannot afford to cut DR. The cost of a disaster both from a monetary and perception standpoint can be incalculable. It's not a matter of IF, it's a matter of when. In IT, any number of things can happen from malicious software to a simple mistake, and companies that have a tried and tested DR plan in place can weather these issues without incident.

Journey to the Cloud

Many organizations use DR as a stepping stone to more permanent cloud offerings such as Infrastructure as a Service (IaaS). When evaluating your cloud DR strategy, during testing or failover, you can see how your systems will perform and behave in a cloud-based environment. Most of the time they will perform as well as, or better than, they do on-site and can help ease into the transition to cloud for not just DR but more IT projects.



Discover the iland Difference

BaaS

iland offers cloud-based backup to adhere to your goal of 3-2-1 resiliency. Leveraging encrypted communication and application trusted tunnels, this off-site, "air-gapped" version of your backup will be available to you if something were to happen to your local recovery. You can recover entire virtual machines, applications or files directly from the cloud.

DRaaS

With DRaaS, iland enables organizations to meet their disaster recovery needs without requiring a secondary data center, additional hardware or even additional staff. With industry leading disaster recovery software and very tight RTO and RPO available, you can be assured that in any disaster (ransomware included) you can bring your environment online quickly with virtually no disruption.

IaaS

Organizations running their workloads in the iland Secure Cloud have peace of mind that security and compliance are always our priority. We uphold a variety of global certifications and standards. So, no matter what industry and region you work in, we have ensured that the proper controls are in place. Coupled with built-in security reporting around vulnerability, network intrusion, malware and virus scanning, you can rest assured that the iland cloud environment is as robust as your own.

Object Storage

Seamlessly extend your on-premises storage to the cloud and efficiently secure and manage your data for long-term retention of business and mission-critical data. Built for resilient digital businesses, iland Secure Cloud Object Storage offers industry-specific security and compliance, guaranteed availability and all-inclusive pricing. Managed through the iland Secure Cloud Platform, iland delivers an integrated experience with our other data protection services such as DRaaS and BaaS for a streamlined experience.

Office 365

Your Office 365 emails and documents are safe and protected with iland Secure Cloud Backup for Office 365. It directly integrates with Office 365 to provide flexibility in how you protect your Exchange Online, SharePoint Online, and OneDrive data. You can quickly restore your mailbox items directly to your Office 365 mailbox by exporting them to a PST file, emailing them as an attachment, or save them locally. This provides protection from deletion and data loss, gaps in retention policy parameters, Malicious insiders, and departing employees.

iland's world-class support is there with you for every step of your journey. Our indepth, consultative sales and onboarding processes ensure that you are as comfortable with your new cloud environment as you are with your own data center. iland support is always included and available by phone or through the iland Secure Cloud Console. iland engineers can help you with everything from managing DNS to invoking backup recovery and DR.

Our Customer's Success Can Be Yours To

East THAMES
Part of the L&Q Group

East Thames

London-based East Thames housing association adopted a cloud-first policy to support the digitization of their business and overcome the barriers of the legacy technology they had in place.

Disaster Recovery a Top Priority

Their incumbent DR solution had very high operational costs, was untested and would require significant capital investments to make it fit for purpose. The IT team was required by the Business Continuity steering group to prove the ability to recover IT systems in the event of a disaster.

Putting Trust in the Cloud

After a thorough investigation, East Thames chose iland Secure DRaaS with Zerto to replicate their data at the hypervisor-level and keep an up-to-date copy of their virtualized applications in iland's cloud. The team was thrilled with the Recovery Time Objectives (RTO). With the old DR solution, recovery times were measured in days and weeks, whereas with iland DRaaS, they are now achieved in mere minutes.

"We made a very good decision to choose iland—their DRaaS solution gives us the flexibility to perform partial failovers of VMs with no configuration changes required which other solutions simply didn't offer."

–Marek Wisniewski, *Head of Technical Infrastructure*

R'Club

R'Club Child Care strengthened their business continuity strategy to ensure that they would be able to care for children of first responders. Downtime during a disaster, like a hurricane, was not an option for this Florida-based nonprofit.

Disaster Recovery a Top Priority

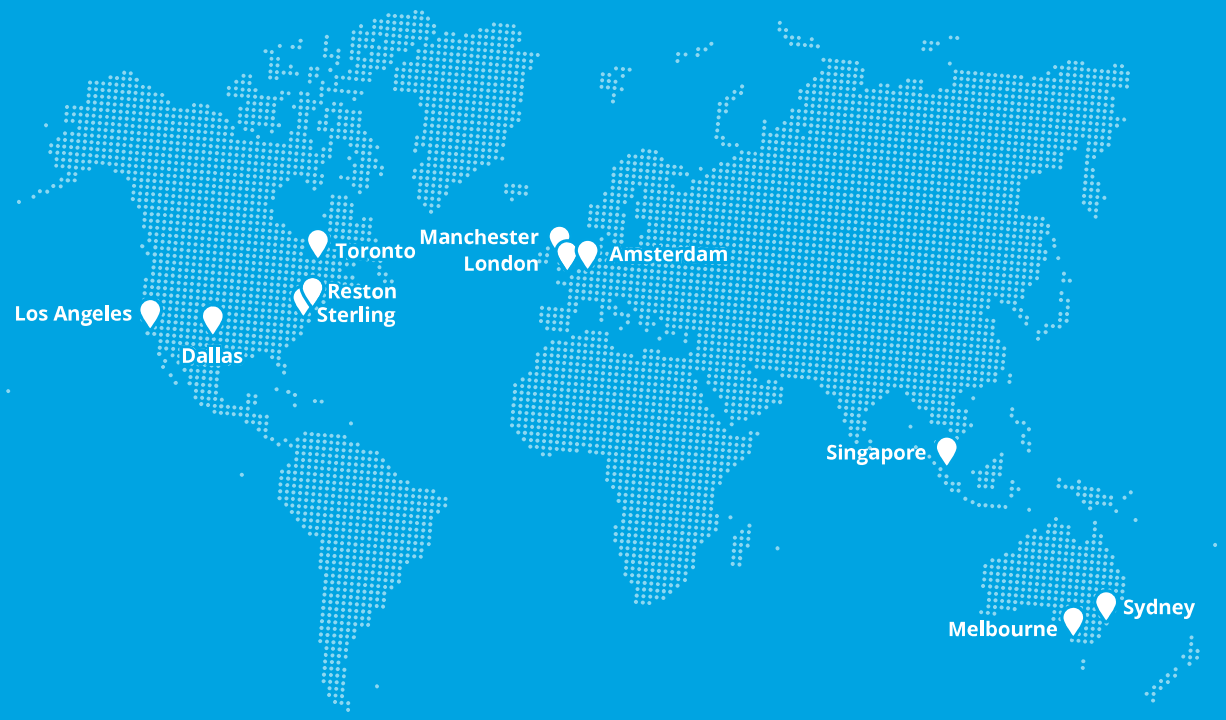
After a poor experience using a cumbersome and inefficient NAS device to copy their Veeam backups off-site, R'Club knew they needed to improve their business continuity plan. They began to research disaster recovery alternatives, keeping cost in mind as their nonprofit budget didn't have funds to spare.

Putting Trust in the Cloud

R'Club wanted to continue to leverage Veeam because they were familiar, and happy with the backup product. After learning more about the capabilities of iland Secure DRaaS with Veeam, the organization knew that was the route for them. Not only did they get to continue using Veeam, but with iland, a Veeam Platinum Cloud Service Provider Partner, replication could begin immediately and the clear pricing and support gave R'Club the confidence they needed in a business continuity solution.

"Having a 'warm site' at iland gives us more security. We know we can continue to operate and provide services to our first responders and our community."

–Michael Brunner, *IT Coordinator*



Thank you.

About iland

iland is a global cloud service provider of secure and compliant hosting for infrastructure (IaaS), disaster recovery (DRaaS), and backup as a service (BaaS).

They are recognized by industry analysts as a leader in disaster recovery. The award-winning iland Secure Cloud Console natively combines deep layered security, predictive analytics, and compliance to deliver unmatched visibility and ease of management for all of iland's cloud services. Headquartered in Houston, Texas, London, UK, and Sydney, Australia, iland delivers cloud services throughout North America, Europe, Australia and Asia.

North America: +1.800.697.7088
UK: +44 20.7096.0149
Netherlands: +31 10.808.0440
Singapore: +65 3158.8438
Australia: +61 2.9056.7004

Learn more at iland.com

iland