verinext

SOLUTION BRIEF

THE TOP SEVEN BENEFITS OF DISASTER RECOVERY-AS-A-SERVICE

Backup and disaster recovery (DR) processes have long been the bane of IT's existence. They absorb enormous amounts of time, energy and budget yet when push comes to shove, they often fail to deliver on their promise of data recovery.

No wonder Disaster Recovery-as-a-Service (DRaaS) has grown so much in popularity in recent years. DRaaS takes advantage of the cloud to streamline and simplify the delivery of DR to the enterprise. Growing at 37% per year, the DRaaS market is expected to be worth more than $11 billion globally by the end of 2023.

Here are seven of the top benefits of DRaaS and the key reasons you may want to consider applying DRaaS in your overall data protection strategy:

1 GREATLY REDUCED TIME AND EFFORT

DRaaS eliminates the need to babysit nightly and weekly backups, deploy a DR site as a mirror image of the corporate data center or refresh expensive equipment (in-house and at the DR site) every few years.

Such activities can hinder IT Operations for days or even weeks on end. They take a long time to set up and somehow never get to the point where they run almost automatically without serious effort. And when a disaster or malware attack strikes, IT can become so embroiled in remediation activities that they have little time for anything else.

For some, the IT talent crunch is so bad they can't afford the skilled data protection and cybersecurity resources they need to safeguard their systems. As a result, critical functions get neglected due to lack to people to take care of them. That's one of the reasons why backup schedules fall behind, why DR best practices aren't implemented and why recovery has become such an uncertain activity.

A managed DRaaS service takes away all the heavy lifting. IT is no longer immersed in troubleshooting backups, maintaining a DR infrastructure or ignoring other urgent projects to deal with the latest data recovery emergency.

2 LOWER DR BUDGETS

Some organizations spend a fortune on DR hardware, software and services. Understandably, many have reduced their DR spending out of necessity. They can't afford to invest as much in DR as they once did. Another element of the DR financial equation is that procurement costs for building DR infrastructure only account for 20% overall. The other 80% is absorbed in maintenance, hardware replacement, troubleshooting, software updates, data migration, backup, and more.

The solution implemented by some organizations has been to send data into the cloud and hope for the best. But in the event of a disaster, outage or ransomware attack, that approach is often revealed to be a false economy. DR is a vital aspect of modern IT that cannot be neglected – yet traditional DR is too pricey for many.

Managed DRaaS solves the dilemma in several ways. It makes effective DR affordable for all. Instead of heavy upfront costs to establish a DR infrastructure and then endless budgeting to maintain that infrastructure, the provider takes care of the underlying hardware and software as well as its ongoing maintenance and support costs. The customer only pays a monthly fee for DR services and support to ensure they can recover when needed. The DRaaS model then eliminates the burden of the costs incurred across the lifetime of the infrastructure. Instead of paying upfront for hardware and software and then paying IT personnel to manage and maintain the desktop infrastructure, everything is available for one low monthly fee, which reduces infrastructure and IT management costs, while helping businesses to avoid costly capital expenditure (CAPEX) and hardware refresh costs.

3 FREQUENT TESTING AND VALIDATED RECOVERY

Testing is always cited as a DR best practice. But it is not always executed successfully. Some only test their plans once a year, but many others pay lip service to testing. They draw up DR plans to activate in the event of a disaster which then lie forgotten in a file cabinet. When disaster strikes, these plans turn out to be woefully inadequate – if they can find them. Embarrassing examples include the hard copy DR binder being in an office that no one could get to, no available list of personnel phone numbers, the DR site being hit by the same event as the primary data center and backups being incomplete or corrupted.

Managed DRaaS provides assurance that DR processes and technologies will dovetail to bring about actual and speedy recovery. Customers can see evidence of testing and validation, so they are certain of the reality of recovery. This includes application and end user testing as well as scenario- or event-based testing whereby a common situation is simulated to validate recovery. Further, DR plans and systems can be tested over and over. As organizations are using a provider, they no longer have to distract internal personnel for lengthy testing drills.

4 ULTRA-LOW RECOVERY POINT OBJECTIVES

The Recovery Point Objective or RPO is a measure of how much data loss is expected or tolerated in the event of a disaster. For example, a disaster occurred at 8 a.m. before anyone came into work and a full backup was done the previous night starting at midnight. In that instance, almost no data would be lost. The RPO would be about eight hours i.e., any data stored by midnight would be saved. But what if the last backup was done the week or month before? The RPO would be measured in days or sometimes weeks. Any data stored between that last backup and the event would be lost. Hence, organizations implement various approaches to reduce their RPO such as snapshots. Implemented correctly, snapshots can take an RPO down to an hour or two. But the lower the RPO, the higher the cost. Many find it challenging or lack the budget flexibility to achieve the RPOs they desire.

The latest services available from managed DRaaS can provide an almost instant RPO. If the organization's security defenses are breaches, if a ransom is demanded, if the power goes out or weather wreaks havoc, a near zero RPO means virtually no data is lost and the organization can be back up and running almost immediately.

5 ULTRA-LOW RECOVERY TIME OBJECTIVES

Recovery Time Objective (RTO) is similar to RPO. It measures of how much time elapsed between the outage and recovery. Like RPO, the lower the RTO, the higher the cost. As a result, some organizations provide low RTOs to only a small subset of their data limited to mission-critical systems. In that scenario, the CRM system might be up and running in an hour or so, but other systems might have to wait days because they aren't as well protected.

Managed DRaaS makes it possible to provide low RTOs to all data and applications at a reasonable cost. Because the cost of the underlying hardware, software and skillsets serve multiple customers, economies of scale make DRaaS-based low RTOs within reach of everyone.

6 HEIGHTENED DISASTER READINESS

Disasters used to be almost exclusively physical events. The weather might lead to a hurricane or a flood. Or there might be an earthquake or a sudden cold spell bringing down the electrical infrastructure. These events were rare. Many organizations never suffered from them, or the event was minor such as power loss for a day or so. Thus, it was possible in the past to hope for the best, not invest much in DR and bet on the odds of never experiencing a disaster.

Those days are long gone. Disasters are more common than ever. Local power outages are becoming far more common due to weather, wildfires and electric grid instability. Floods, hurricanes and unexpected hot or cold snaps appear to be rising in frequency. To make matters worse, ransomware- and malware-based outages have taken over as the number one reason for downtime. If cyber-gangs infiltrate the network, they can shut everything down, disable or corrupt backups, encrypt all data and hold the organization to ransom.

IT in the modern world needs comprehensive DR protection. And managed DRaaS is the best way to provide it broadly. Whether for SMBs that lack the personnel and resources to address DR or large companies that would rather focus IT on more strategic business initiatives, DRaaS opens the door to rapid recovery no matter what. DR-as-a-Service also typically has built-in security features that are far more extensive than those available in most organizations. Clients receive monitoring by trained personnel who are constantly on the lookout for anomalous behavior, misuse of ports, or other signs of an ongoing or imminent attack.

7 MULTI-CLOUD PROTECTION

Modern organizations now have workloads on-premises, in the cloud and in multiple clouds. Their infrastructure is more complex than ever. Those trying to manage backup internally often run into this wall of complexity. If backups are thorough, they typically take up far too much internal time. But many times, certain applications, data sets and systems are omitted from the backup schedule.

Managed DRaaS moves all this complexity from IT into the hands of an external provider. All the business needs to do is spend a small amount of time to verify that all data is covered.

PUT YOUR DR IN THE HANDS OF THE PROFESSIONALS

The Verinext DRaaS Managed Service is powered by the HPE GreenLake secure edge-to-cloud platform. Leveraging the power of Zerto for ransomware protection and disaster recovery for any app, the Verinext DRaaS Managed Service offers the industry's lowest recovery point objectives and fastest recovery time objectives. Delivering real-time protection and near-zero data loss and application downtime, the DRaaS solution supports rapid time to deployment, predictable consumption-based costs and is fully managed, 24/7 by Verinext experts to assure continuous data availability, security and recovery readiness.

verinext

With Verinext DRaaS Managed Services, customer data has a dedicated retention solution and comes complete with rapid onboarding and rapid recovery services that meet even the most stringent SLAs.

For more information visit verinext.com/services/managed-services