SEGRA

The Advantages of a Private Fiber Network for Your DRaaS Strategy

Protecting your business data as part of a well-designed business continuity plan has never been more complex or important. Disaster recovery (DR) is an essential part of planning. Creating a DR strategy helps ensure that your business can return to full functionality after an attack. It differs from business continuity plans that identify prevention and recovery methods to deal with potential threats.

As part of the growing migration to the cloud, a modern disaster recovery strategy involves Disaster Recovery as a Service (DRaaS). When deployed, DRaaS mitigates downtime due to outages because it allows organizations to connect to a cloud data center the same way they would connect to a physical data center's resource. You are protected against downtime because the cloud data center keeps data in a live state.

When deployed, DRaaS mitigates downtime due to outages because it allows organizations to connect to a cloud data center the same way they would connect to a physical data center's resource.

Challenges Moving Data to the Cloud

Bandwidth

How do you get data to the cloud quickly and securely? Replication—the synchronous replication of virtual machines (VMs) from the network infrastructure to the target DR site—is the most common method in disaster recovery. This requires the bandwidth to ensure fast and reliable communications, so that changes to a VM also occur at the target site.

However, consistent, reliable bandwidth is one of the biggest challenges for disaster recovery. During the pandemic, many work teams are used to video transmission freezes during meetings. But when you need to transmit full datasets for replication, transmission stalls can have a critical impact on the integrity of your data.

Security

Many organizations need DR sites with an equal or higher level of security than their own infrastructure to meet compliance and regulation requirements. Maintaining and demonstrating compliance can be difficult in public cloud environments if you are working with multiple providers who have different service-level agreements.

Costs

For organizations using the public cloud for disaster recovery, migrating and hosting petabytes of data can come at considerable cost. Data-intense applications require an extremely fast network that raises the expense of using a public cloud service. A public cloud DRaaS might seem to be a low-cost option, but after configuring the CPU and RAM needed for recovery and factoring in costs for bandwidth, accessing data, stored capacity, resilience, and retrieval frequency, the actual costs add up.

The Resilience and Efficiency of Private Fiber Networks

Downtime due to data breaches or non-compliance can cripple a business. According to Gartner, the average cost of network downtime is $5,600 per minute. Plus, there are costs that often don't show up in dollar form, such as the cost of diverting your IT department from important projects and responsibilities that contribute to the growth and well-being of the organization, to managing an outage.

Recovery time objective (RTO), the amount of time it takes to recover normal business operations after an outage, and recovery point objective (RPO), the amount of data you can acceptably afford to lose in a disaster, are key metrics in evaluating data recovery solutions. A dedicated private network offers faster, more reliable connectivity than the public cloud, and provides the resiliency necessary to ensure data integrity and speed to meet the most demanding RTO and RPO.

Additionally, for organizations that handle sensitive data or are subject to data privacy regulations, a dedicated private network is a more secure option for DRaaS cloud services. Data that moves across a dedicated private network is not accessible to anyone outside the private network while in transit and therefore doesn't require encryption. Public networks require encryption, a necessary overhead that reduces speed. In contrast, a private network is completely isolated from the public internet.

Segra's DRaaS Solution Enables Efficient Recovery

Segra's private cloud solution is a private fiber network that allows live replication to and from its data centers so customers can fully recover mission-critical data. To ensure fast recovery from disruptions, Segra's standard service levels have an RPO of seconds and RTO of minutes.

Recovery speed is critical in disaster recovery. With new and evolving threats, it's important to be able to roll back data quickly, which a private cloud can do. If you're using a public network and your RPO is in hours, you've reduced the number of times you can roll back your data. Segra's DR utility creates a journal entry every 5-10 seconds, which lets you easily roll back to those journal points and recover files, applications, and VMs at specific points in time. If you experience a ransomware attack and can determine when it occurred, you can use the journal points to quickly roll the state of your infrastructure back before that period.

Segra's DRaaS solution keeps your data in a live state. VMs are replicated and online so you can recover an application or the entire VM at another location while keeping other services up and running at your primary data center.

Retaining data for a longer period allows you to recover rapidly. If you only use a backup utility, it can take much longer. For example, if you only relied on backup and experienced a ransomware threat, you would have to roll back to your last backup. A data loss of one week could take three to four days to recover. Segra's DRaaS solution keeps your data in a live state. VMs are replicated and online so you can recover an application or the entire VM at another location while keeping other services up and running at your primary data center.

Providing Data Integrity, Speed, Efficiency, and Security

Segra can help customers overcome bandwidth challenges because our fiber infrastructure network is over 30,000 miles and connects more than 10,000 locations and nine data centers. As one of the largest independent fiber infrastructure bandwidth companies in the eastern US, Segra can provide customers with the fiber connectivity they require for DRaaS.

Segra's solution is storage agnostic. It supports mixed hypervisors and can replicate any data center or site, including private cloud, public cloud, service provider or branch office. If you prefer a hybrid cloud solution, Segra can connect a private fiber connection across the Segra fiber network to the public provider. Your data is kept private, and you experience consistent performance while reducing data loss and maintaining security.

Segra's world-class data centers meet the strictest industry standards and are compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Statements on Standards for Attestation Engagements (SSAE), and the Payment Card Industry Data Security Standard (PCI DSS). All Segra facilities are SSAE 16 SOC 2 Type II-certified and are monitored continuously.

If you have a high data change rate for VMs, databases, and applications, bandwidth is always a concern, and a private network is going to be more advantageous than a public cloud solution. With a robust feature set, long-term retention, and continuous replication at the virtualization/hypervisor layer, Segra's DRaaS solution delivers a high-performance disaster recovery and archival solution. Combined with its extensive fiber network, the Segra DRaaS solution provides end-to-end security and reliability.

To learn more about Segra's DRaaS solution, go to **www.segra.com/business** or call **833.GO.SEGRA.**

SEGRA

833.GO.SEGRA
businesssolutions@segra.com
www.segra.com