veeam ProPartner Network



The Service Providers' Path to Exceptional DRaaS with Veeam

veeam ProPartner Network

Contents

Introduction	**3**
Meeting Backup and Replication Needs	**4**
Expertise in Disaster Recovery Planning: Resource Augmentation	**5**
What is DRaaS?	**6**
Traditional DR vs. DRaaS	6
Cloud-Based DR: Public Cloud and Service Provider Data Center	6
Use Cases for DRaaS Beyond Disasters	**7**
Partner Considerations for Building a DRaaS Offering	**8**
Consulting and Business Impact Analysis (BIA)	9
Leveraging Multi-Disciplinary Expertise	9
Providing a Unified Management Console	9
Testing and Maintaining the DR Plan	9
Determining the Level of Management the DRaaS Offering Will Provide	**10**
Self-Service	10
Assisted Recovery	10
Fully Managed	10
How Business Recovery Objectives Drive DRaaS Technology	**11**
How Veeam can Help Providers	**13**
Veeam-powered DRaaS Specs	**14**
Veeam Cloud Connect	14
Support for snapshot-based replication and CDP	14
Test failover functionality	15
Network extension appliances	15
Veeam Service Provider Console	15
The VCSP Program	**16**
Veeam Recovery Orchestrator	16
Tackling Service Provider and Customer Needs with Veeam-powered DRaaS	**17**

Introduction

As the volume and importance of data continue to grow, mitigating the growing potential for data loss has become a top priority for every organization. The complexity of disaster recovery has naturally given rise to disaster recovery as a service (DRaaS) so that organizations can rely on skilled partners to protect against potential catastrophes.

However, for service providers, choosing the right DRaaS solution and approach can be challenging in a digital world where they must fully understand what end users need.

With data survivability being primary goal, every business has a long list of data vulnerability challenges, such as ransomware attacks, that they must confront proactively. In 2022, 85% of organizations experienced a ransomware attack, with just 45% of encrypted or destroyed data able to be recovered, according to the Veeam Data Protection Trends Report 2023.

As to how long it took to bounce back after an incident, 30% of organizations answered one to two weeks, but 35% said it took two weeks to a month in Veeam's Ransomware Trends 2023 report. This vulnerability to attack, along with backup and DRmitigation, is often made more difficult by a host of challenges, including:

- The need for near-zero downtime to maintain operations based on business data dependency.
- Legacy methods of having a secondary backup data center is far too expensive, rigid, and inefficient to ensure the protection of data and systems.
- The data sprawl across on-premises, virtual, cloud, and SaaS applications and workload data distribution.
- Regular updating and supervision required for backup and DR system data.
- Constant infrastructure evolution that requires frequent testing to ensure all environment changes in the backup and DR system are updated.

In 2022, 85% of organizations experienced a ransomware attack, with just 45% of encrypted or destroyed data able to be recovered

These reasons require many large and small end-user customers to depend on service providers to manage their business resiliency strategies and provide a comprehensive service.

That's one reason why most businesses ranging from small- to medium-sized businesses (SMBs) to global enterprises have long since passed the time when they could effectively set up and manage a backup and DR system on their own. It's also why providers must deliver a solution that clearly addresses each specific intricacy of system relationships, applications, and workload restoration sequences.

This includes meeting demands for the lowest recovery time objectives (RTOs), agile recovery point objectives (RPOs), and the ability to offer DRaaS solutions that can address both high availability and DR, which are both varied and complex. These needs require a highly agile and comprehensive BaaS and DRaaS data protection solution that can fit the needs of a wide variety of end users.

 © 2023 IOD Cloud Technologies Research Ltd. Reproduction in whole or in part without written permission is prohibited.

Meeting Backup and Replication Needs

There are many challenges inherent to backup and replication, which are often confused as being the same thing. These related but non-interchangeable processes have critical distinctions and outsized challenges for businesses and providers who rely on backup only.



RPO: How often the backup is created (usually once a day, which means losing up to 24 hours of changes).



Impact on production infrastructure: The backup may take several hours and affect the performance of backed up workloads.



RTO: The maximum length of time a system can be down. This can be affected by the performance of the media and where backup data is stored.



Onsite or offsite availability of backup media, in case the production site is down.



Ability to have point-in-time recovery: If the database is being backed up alongside transaction logs.



Recovery location: Whether the production site is available to restore, or a secondary site is needed.



Networking connectivity: If data is being restored offsite, it's important to know how to re-establish connections to the failover site in the proper order to ensure business continuity.

Data backup alone can risk data loss between backups if not managed and monitored correctly. This method is still an overall industry standard for countless businesses that must store large sets of static data for compliance.

Data replication fulfills a vital piece of the recovery puzzle in terms of business continuity. The goal is to deliver continuous operation of mission-critical applications and workloads after a disaster. This process requires duplicating and synchronizing data across an organization's locations and environments that range from servers and virtual machines (VMs) in data centers to cloud environments. There are two main types of data replication:

- **Near-synchronous** Continuous Data Protection (CDP) replication
- **Snapshot-based replication** where data replication happens at set time intervals, which introduces brief latency after initial savings and consumes less bandwidth and time than synchronous replication.

Providers today must deliver comprehensive services solutions that deliver both backup and data replication to accommodate the needs of every business and situation. This can range from backing up everything (i.e., servers and desktops) to providing replication for mission-critical applications.

 © 2023 IOD Cloud Technologies Research Ltd. Reproduction in whole or in part without written permission is prohibited.

Expertise in DR Planning: Resource Augmentation

Organizations often face challenges in garnering the expertise needed to build, maintain, and execute backup and DR on their own. Resource augmentation through DRaaS provides access to a pool of specialized professionals who can tailor DR plans to specific business needs, which ensures that businesses account for all critical systems. This can include the development of ransomware response and playbook development support for faster implementation and coordination.

Experts can leverage deeper knowledge of their latest DR technologies and best practices to offer faster and more proactive maintenance and execution (in the event of an incident) for the DR plan.



 © 2023 IOD Cloud Technologies Research Ltd. Reproduction in whole or in part without written permission is prohibited.

What is DRaaS?

DRaaS is a cloud-based service model that delivers replication and physical or virtual server hosting for failover purposes if a disaster affects the original data center repository. This differs from traditional DR approaches since it offers a more flexible and cost-effective solution that avoids physical infrastructure investment.



Traditional DR vs. DRaaS

While traditional DR often involves setting up and managing a complex and expensive secondary DR site like a second data center, DRaaS uses the provider's infrastructure. This eliminates the need for a dedicated physical site and reduces capital expenditure while being scalable and adaptable to each end user's changing needs.



Cloud-based DR: A Public Cloud and Service Provider Data Center

Cloud-based DR includes options for both public cloud and service provider data centers by leveraging public cloud infrastructures. Service providers offer DRaaS as a managed service by using their datacenters that are tailored to the needs of each individual business with dedicated support.

 © 2023 IOD Cloud Technologies Research Ltd. Reproduction in whole or in part without written permission is prohibited.

Use Cases for DRaaS Beyond Disasters

DRaaS has several other use cases beyond recovering from natural or cyber-related disasters, including:

- Simplified, regular, and non-disruptive **DR plan testing** that enables failover mechanisms to ensure recovery procedures are effective and up to date.
- **CDP point-in-time capabilities** for recovering files and folders in seconds.
- **Seamless migration of data** and applications to the cloud or as part of a transition between data centers.
- The ability to perform regular DR testing and recover data within **specific time frames** to meet regulatory compliance.
- Meeting peak demand periods via **short-term capacity expansion** without investing in additional infrastructure.

These collective DRaaS elements give providers a far more comprehensive solution for business continuity that addresses both traditional disaster scenarios and broader operational resilience needs. While the benefits of DRaaS may be clear, each organization must have a comprehensive understanding of its needs to find the right service provider with the right solution.

 © 2023 IOD Cloud Technologies Research Ltd. Reproduction in whole or in part without written permission is prohibited.

Partner Considerations for Building a DRaaS Offering

In 2023, 24% of organizations are using multiple self-managed data centers for BC/DR, with 47% using cloud infrastructure or a DRaaS provider. That cloud/DRaaS number is expected to jump to 55% by 2025.

However, finding the right vendor technology partner like Veeam, who has the best solutions for building the ideal DRaaS environment, has several key steps. All these steps put the burden on the provider to be able to deliver and customize their services to meet each customer's needs.



 © 2023 IOD Cloud Technologies Research Ltd. Reproduction in whole or in part without written permission is prohibited.

Consulting And Business Impact Analysis (Bia)

The provider must be able to usher each client through a comprehensive and easily understood consulting process that delivers a comprehensive business impact analysis (BIA). This helps providers understand each client's priorities, needs, and pain points along with the systems that support mission-critical business processes.

A BIA informs the design of a DRaaS plan so that it aligns with the client's operational objectives and risk tolerance.

Leveraging Multi-Disciplinary Expertise

Since DRaaS extends well beyond the scope of a traditional backup, it requires a multi-disciplinary approach that involves expertise in:

- **Networking** that ensures reliable connectivity between the client's primary site and DRaaS infrastructure, especially during failover operations.
- **Cloud technology and environments** that support the provider in choosing and leveraging the best scalable and cost-effective DR solutions.
- **Hardware** to bring a deep understanding of the physical requirements for storage and compute resources in a DR scenario.
- **All aspects of software** and how it can be integrated and managed as critical DR components along with replication and orchestration tools.

Providing A Unified Management Console

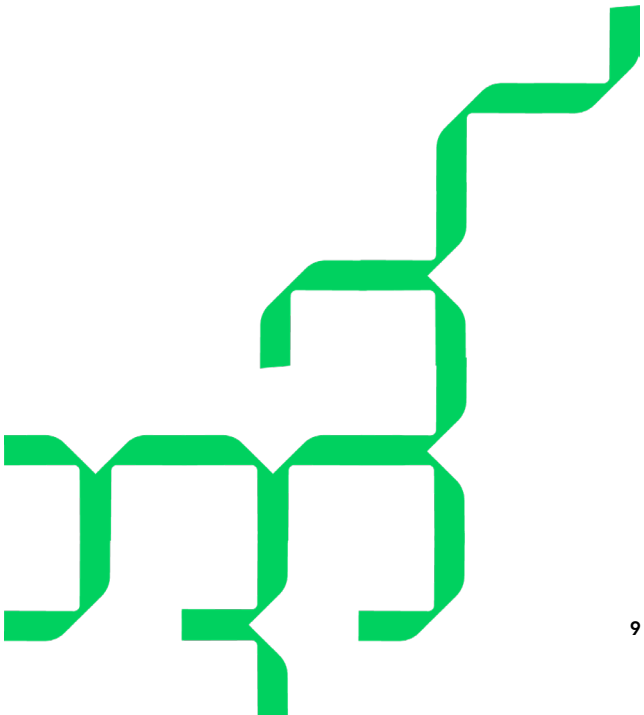
Each client must have an easily understandable and unified management console that can deliver a seamless DRaaS user experience by offering:

- Clear insights into the replication status, system health, and readiness for failover
- Easy-to-use controls for initiating failovers, failbacks, and recovery workflows
- Compatibility with existing management tools and platforms in ways that simplify the user experience

Testing And Maintaining The Dr Plan

Regular testing of DR plans is crucial to ensure effectiveness, which is why partners should provide:

- **Available and automated DR testing** tools to reduce burden on client resources
- **Plan maintenance** for continuous updates to DR plans as the client's IT environment and business needs evolve
- **Detailed reporting** on testing outcomes, encountered issues, and improvement recommendations



 © 2023 IOD Cloud Technologies Research Ltd. Reproduction in whole or in part without written permission is prohibited.

Determining the Level of Management the DRaaS Offering Will Provide



Self-Service

This scenario is when a customer leverages the infrastructure and tools offered by their DRaaS provider for certain responsibilities. These tasks can include activating and shutting down recovery configurations, failover and fallback procedures, and replicating VMs.



Assisted Recovery

In assisted DRaaS, the customer initiates the recovery procedure when disaster strikes. Meanwhile, the provider will offer support by way of overseeing the recovery infrastructure and handling data replication.



Fully Managed

Fully managed DRaaS works best for IT teams who lack the in-house time and expertise to manage DR. The DRaaS provider implements, manages, and executes the DR plan, and also manages the failover and fallback processes. This includes all other processes associated with running a DR environment.

A successful DRaaS offering requires providers to surpass traditional IT roles and provide comprehensive consulting, diverse technical expertise, seamless management experience, and rigorous testing and maintenance protocols.

By addressing these considerations, provider partners can build a DRaaS solution that not only safeguards against disasters, but becomes an integral component of their clients' operational resilience.

 © 2023 IOD Cloud Technologies Research Ltd. Reproduction in whole or in part without written permission is prohibited.

How Business Recovery Objectives Drive DRaaS Technology

The technology that underpins the ideal DRaaS solution is driven by business recovery objectives that ensure business continuity. This makes it critical for providers to understand the nuances of different DRaaS technologies and how they align with recovery objectives for tailoring services to meet specific customer needs.

Veeam's 2023 "Cloud Protection Trends" report shows that 46% of organizations choose to self-manage their backup jobs while relying on a BaaS/DRaaS provider to maintain their backup servers and services. This is one reason DRaaS comes in a few different flavors depending on user needs and the service requirements of each IT department. This includes self-service to fully managed services, which were covered in the previous section about partner considerations.

While self-service and assisted recovery give clients complete or partial control with the ability to fine-tune their services, most clients will opt for fully managed DRaaS. The challenge for providers is to deliver the right technology solution that meets a wide variety of business recovery objectives. These technologies include:

1. **Backup technology** that's capable of creating periodic data snapshots for restoration in the event of data loss. This is often used for non-critical data with longer RTOs.

2. **Replication technology** to provide near real-time copying of data to a secondary location. This is essential for mission-critical applications where data loss cannot be tolerated and RTOs are short.

3. **CDP** for real-time data capture and storage with the ability to restore to any point in time, including folder- and file-level recovery with the same benefits. This is ideal for extremely critical data where even minimal data loss could have significant business impact.

A staggering 82% of organizations say they have an availability gap between their needed and actual recovery speeds for returning full user productivity. That's why most organizations require a comprehensive approach to backup and DR from a service provider andpartner that can deliver BaaS with DRaaS functionality in a single, agile data protection solution.

BaaS delivers cloud backup software to replace onsite hardware, software, and servers that are managed by the provider. With DRaaS, a replication of the customer's environment is hosted in the cloud to deliver failover and failback capabilities, which requires effective backups. This also requires the expertise to:

- Understand the specific resources and applications that must be brought back online first.
- Save any changes in data during the failover period.
- Failback to the main production site once restored along with any data changes.

 © 2023 IOD Cloud Technologies Research Ltd. Reproduction in whole or in part without written permission is prohibited.

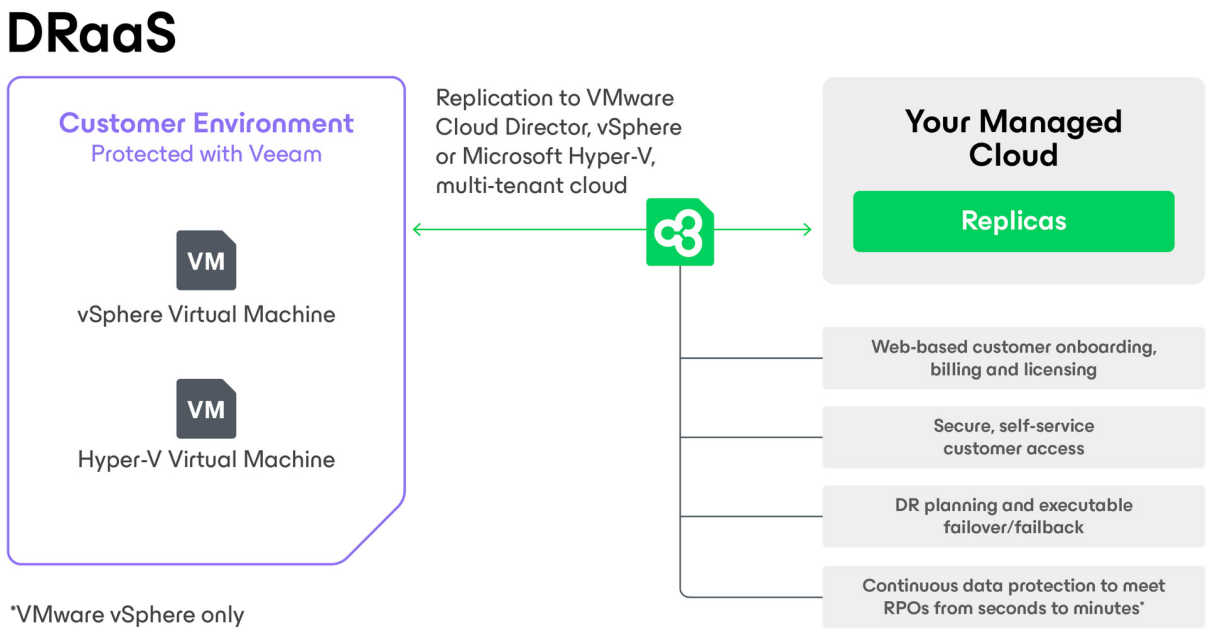
In other words, the ideal solution from a provider will need to offer each customer backup, replication, and CDP. This enables the provider to support varied:

- **SLAs** based on RTOs and RPOs, with backups for longer RTOs and RPOs, replication for medium ones, and CDP for the shortest SLAs.
- **Workload tiering** for data and applications based on their criticality, with each tier having a tailored recovery strategy that uses one or a combination of these methods.

Most customers will want to use CDP judiciously since this level of unparalleled data protection isn't necessary for all data types and can significantly increase costs. This enables the provider and customer to evaluate the criticality of their data to determine if CDP is warranted. They can then choose a DRaaS plan that aligns with their actual requirements and avoid the expense of over-insuring non-critical data.

While this is a tall order for most providers and very difficult to find in a single solution, Veeam Backup & Replication offers such a wide spectrum of necessary data protection methods that range from backup and replication to CDP.

Let's see how Veeam can help providers deliver the level and type of DRaaS that delivers a cost-effective, customized solution that precisely meets the recovery needs of each customer.



 © 2023 IOD Cloud Technologies Research Ltd. Reproduction in whole or in part without written permission is prohibited.

How Veeam can Help Providers

As businesses increasingly rely on virtualized environments, the need for effective DR solutions becomes absolutely paramount. Nearly half (46%) of organizations intend to use cloud services as their DR site, which includes cloud infrastructure and DRaaS. That's one of many reasons why Veeam offers technology and programs that enable providers to implement a robust DRaaS strategy for their customers with the ability to affordably scale.

Veeam's approach to DRaaS enables partners to deliver high-quality offsite backup and DR solutions and outcomes to organizations. Veaam's state-of-the-art tools give partners the ability to leverage the strengths of backup, replication, and CDP in a single platform. This offers world-class protection to customers via a robust service offering that's supported by service providers and powered by Veeam.



 © 2023 IOD Cloud Technologies Research Ltd. Reproduction in whole or in part without written permission is prohibited.

Veeam-powered DRaaS Specs

Veeam Backup & Replication provides backup, recovery, and replication for critical workloads including VMware (i.e., vSphere to vSphere and CDP, vSphere to VCD along with CDP) and Microsoft (i.e, Hyper-V to Hyper-V) among others. Veeam Backup & Replication, including Veeam Cloud Connect and Veeam Service Provider Console, is the technology suite that powers DRaaS.

Veeam Cloud Connect

Veeam Cloud Connect allows service providers to create a Veeam-powered service offering for offsite backup and DRaaS. The focus on offsite backup workloads leverages Veeam Cloud Connect, which is essential for being able to keep one copy of your data offsite per the 3-2-1 Rule. This gives providers the power to deliver seamless data storage at an offsite location at no extra cost, which, in turn, encourages customers to engage them as their trusted service provider for safeguarding their digital assets.

Veeam Cloud Connect Replication for DRaaS provides a secure, multi-tenant environment that natively integrates with VMware Cloud Director. Veeam Cloud Connect integrates hosted cloud repositories in a single backup console.

Veeam Cloud Connect allows for the precise failover of VMs or entire sites to enable fast and efficient recovery without disruption. This allows provider/partner customers to include cloud backup infrastructure that is made up of a hosted backup storehouse and comprehensive backup services with no second site management costs or need for a VPN.

In 2022, cyber attacks hit backup repositories 75% of the time, with malicious actors targeting backup repositories at least 93% of the time. Veeam Cloud Connect can air-gap backups with insider protection to protect against ransomware with immutability or insider protection.

Support For Snapshot-Based Replication And Cdp

When planning for DR, Veeam can deliver three options to achieve RTOs and RPOs, including:

- VMware-based and snapshot-based replication
- Storage-snapshot-integrated, subsystem-based replication
- CDP

 © 2023 IOD Cloud Technologies Research Ltd. Reproduction in whole or in part without written permission is prohibited.

Test Failover Functionality

With Veeam, providers can test tenant cloud failover plans to make sure replicated tenant VMs on the cloud host start successfully with external network access after failover. This extends to both partial site and full failovers. In partial site failovers where only one or several production VMs become corrupted, the tenant can quickly recover a corrupted VM by failing over to its replica on the cloud host.

Planned CDP failover functionality is also possible. This can be implemented in advance of a known weather event, testing, or migration scenario.

Full-site failover can be performed in the event of a software or hardware malfunction that leaves the entire tenant production site unavailable. This scenario ensures that all critical VMs failover one at a time or as a group to their replicas on the cloud host.

Network Extension Appliances

Veeam DRaaS includes network extension appliances, which facilitate partial failovers. This allows for DR of selected VMs, which can maintain communication with the tenant's production site to enable greater flexibility and precision in DR operations.

Veeam Service Provider Console

Veeam Service Provider Console gives service providers access to Veeam Data Platform's remote backup, replica monitoring, and reporting across nearly all Veeam products. This comprehensive view of customizable multi-tenant environments automate everything from customer onboarding to licensing and billing so providers can easily scale their business.

Clients rely on their providers to deliver customizable and comprehensive DRaaS that protects their data, applications, and workloads across complex environments. To ensure that provider partners can deliver on the needs of every client, Veeam provides unparalleled support via its Cloud & Service Provider (VCSP) Program.



 © 2023 IOD Cloud Technologies Research Ltd. Reproduction in whole or in part without written permission is prohibited.

The VCSP Program

By supporting service providers through the VCSP program, Veeam enables each partner to deliver the backup and DR services that each client needs while positioning the provider to grow their own client base. The VCSP program offers a wealth of resources for partner providers, including flexible licensing, free tools, sales, technical and marketing support resources, and much more.

To further promote top partner solutions that are built on the Veeam Data Platform, the Veeam Competency Program initiative is designed to support provider competency across its entire global partner network. These VCSP customer-ready competencies recognize partners that provide Veeam-powered "as a service" solutions to customers via existing VCSP competency categories, which include:

- Off-site Backup for Ransomware Resiliency
- Disaster Recovery as a Service (DRaaS)
- BaaS for Microsoft 365
- Managed Service Provider (MSP) Backup (for resellers only)
- BaaS for AWS and Azure

Veeam Recovery Orchestrator

The need to orchestrate recovery workflow processes is critical for any BC/DR strategy or solution. However, Veeam's data protection report revealed that less than 18% of companies currently have this kind of capability.

For partners working with enterprise customers with multiple datacenters, Veeam Recovery Orchestrator delivers orchestration recovery processes that automate recovery workflows for critical applications/workloads with robust documentation and testing features that meet compliance requirements. Built on top of Veeam Backup & Replication and Veeam ONE, Veeam Recovery Orchestrator can do the following:

- Establish recovery orchestration workflows for virtual and physical machines to VMware vSphere and Microsoft Azure cloud environments.
- Automate check and test schedules for orchestration plan verification for things like isolated test labs and comprehensive readiness checks.
- Enable viewing of RPO and RTO achievements on the dashboard and create updated orchestration plan reports for checks, tests, and executions to meet compliance requirements.

Veeam Recovery Orchestrator also provides vSphere VM recovery orchestration based on replicated storage snapshots that were created on NetApp and HPE storage systems. It also offers orchestration plans for vSphere VMs that should be failed over to replicas and CDP replicas. Veeam Recovery Orchestrator can also include vSphere VM and Veeam Agent backups that should be recovered to a VMware vSphere environment or a Microsoft Azure cloud environment.

 © 2023 IOD Cloud Technologies Research Ltd. Reproduction in whole or in part without written permission is prohibited.

veeam ProPartner Network

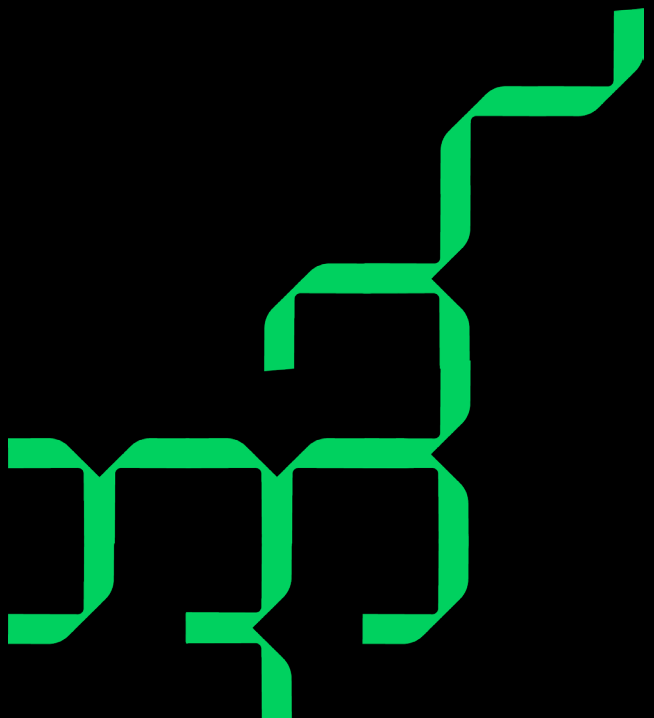
Tackling Service Provider and Customer Needs with Veeam-powered DRaaS

As the data landscape becomes more complex across different systems and cyber security challenges increase, customized approaches to business continuity support become more vital. Veeam-powered BaaS and DRaaS is built to meet the needs of companies that lack the personnel, skills, and resources to design, implement, and manage these backup and DR solutions.

At the same time, Veeam Data Platform was designed to support providers tasked with delivering services to those clients. The VCSP program reinforces providers through support and certifications that help them grow and adapt to each organization's evolving data protection needs.

Veeam protects over 450,000 customers worldwide, including 80% of the Fortune 500 and 72% of the Global 2,000, with future growth predicated on the ability to deliver the right solution and support at the right time. Veeam empowers every organization to achieve radical resilience through data security, data recovery, and data freedom for their hybrid cloud.

Follow these links to learn more about the Veeam Cloud & Service Provider program and Veeam solutions for service providers.



 © 2023 IOD Cloud Technologies Research Ltd. Reproduction in whole or in part without written permission is prohibited.

veeam ProPartner Network

iamondemand.com