VMware Cloud Disaster Recovery for Managed Service Providers

Help customers rapidly recover from ransomware, power outages and other disasters

KEY HIGHLIGHTS

- Instantly power-on your VMs in the cloud when testing or orchestrating your DR plans
- Protect your data from malware thanks to a deep history of immutable snapshots
- Provision a small failover footprint capacity in the cloud and scale on-demand
- Get detailed DR reports to ensure DR plans are being tested and executed correctly
- Minimize failback cloud egress charges and optimize DR operational costs
- DR health checks are automatically run every 30 minutes for increased reliability

KEY USE CASES:

- Recover from ransomware
- Expand or replace existing DR site
- Optimize DR costs
- Audit ready DR
- Remote office/branch office (ROBO) DR

"VMware Cloud Disaster Recovery will allow us offer a robust end-to-end VMware-based DRaaS solution. We can configure all infrastructure environments (including DR environments) with VMware solutions, which should reduce the burden on the customer, by centralizing the support and consolidating billing and payment."

- Kazutaka Goto, Executive Officer / Partner Alliance, iret, Inc

Disaster Recovery (DR) has Become Critical for Every Business

In a recent survey, 76% of respondents reported an incident during the past two years that required an IT Disaster Recovery (DR) plan, while more than 50% reported at least two incidents. At the same time, cyberattacks are on the rise, becoming a top driver of increased business risk. In 2019, 52% of global enterprise network security decision makers had experienced at least 1 sensitive data breach in the past 12 months[1]. It is therefore not surprising that CXOs and board members increasingly care about disaster recovery.

Although many organizations realize the importance of implementing a robust DR solution for reasons including, but not limited to, business continuity, compliance with industry regulations, protection against disasters, ransomware and security breaches, traditional DR solutions can be complex, expensive, and unable to scale or provide the required levels of protection that organizations need.

End Customer Challenges Partners Need to Address

Traditional backup and disaster recovery mechanisms are not sufficient for modern data protection. Over 50% of DR events[2] are tied to localized data center events (Ransomware and Power Outages). Other causes could include natural disasters, human errors, hardware failures, malfeasance, etc. Current DR solutions present the below challenges for end customers:

- **Complexity**: Customers may end up with a multi-vendor approach consisting of different hardware and software elements brought together to provide a workable solution. Bringing multiple product interfaces and consoles to implement, manage, and operate, lacks integration, and increases the operational complexity of the combined solution.
- **Cost**: Traditional on-premises solutions, whether they be secondary data centers or the use of a co-lo facility, are expensive to implement and maintain. The purchase of additional hardware required to implement a secondary location like servers, storage, networking, etc., amplifies the investment required to implement the solution. All the while the goal is to not have to utilize these resources.
- **Predictability**: We know from industry data that only 17% of customers actively test their disaster recovery implementations and plans. That is money being spent on something that customers aren't sure will function properly when the time comes. Add to that the use of multiple vendor products, lack of appropriate testing and validation of the solution which increases the lack of confidence organizations have in the disaster recovery strategy.

1 Forrester, "Top Cybersecurity Threats in 2020", January 24, 2020

2 VMware (Datrium) Survey

"VMware Cloud Disaster Recovery will enable us to offer disaster preparedness that maximizes the benefits of the cloud, specifically to customers looking to steer away from using a data center as a recovery site. VMware Cloud DR will allow them to set up a robust disaster recovery strategy without investments in hardware, equipment, or other operating costs. CTC will continue to support customers' first steps into full-scale cloud utilization by partnering with VMware to deliver robust solutions to address their digital transformation needs."

- Takao Kodama, General Manager, Entrusted Cloud Sales Division, ITOCHU Techno-Solutions Corporation

ON-DEMAND

- Instant power-on (Live Mount)
- Pilot light option
- No VM format conversions
- Rapid ransomware recovery

EASY-TO-USE

- Consistent, familiar operations
- SaaS-based management
- Continuous DR health checks
- Automated built-in audit reports

CLOUD ECONOMICS

- Pay when capacity needed
- Efficient cloud storage
- Simple dollar per TiB pricing
- Optimized failbacks

LEARN MORE

Visit the MSP webpage *here* and the VMware Cloud Disaster Recovery product page *here*. Get discount details *here* and pricing details *here*.

FOR MORE INFORMATION OR TO PURCHASE VMWARE PRODUCTS

Call 877-4-VMWARE (outside North America, +1-650-427-5000), visit *vmware.com/products*, or search online for an authorized aggregator.

The VMware Cloud Disaster Recovery Solution

VMware Cloud Disaster Recovery offers on-demand disaster recovery to IT administrators responsible for IT infrastructure and services resiliency and are faced with the challenge of DR being complex, expensive, and unreliable. It also helps end customer's security and compliance teams, often under the purview of the Chief Information Security Officer, to ensure that operations can resume after a disaster event. Delivered as an easy-to-use SaaS solution with cloud economics, VMware Cloud Disaster Recovery combines cost-efficient cloud storage with simple SaaS-based management for IT resiliency at scale.

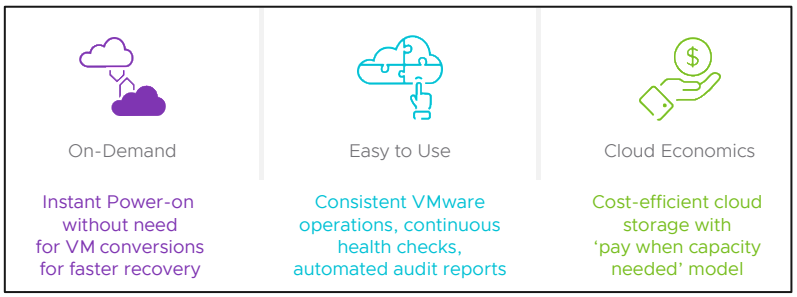

FIGURE 1: VMware Cloud Disaster Recovery Benefits and Capabilities

Partners benefit from consistent, familiar VMware operations across production and DR sites and can offer a 'pay when you need' failover capacity model for DR resources to customers, along with the benefit of instant power-on capabilities for fast recovery after disaster events.

On-Demand

VMware Cloud Disaster Recovery delivers fast recovery with zero copy and no rehydration of data from cloud storage to VMware Cloud on AWS hosts. For achieving production-level performance, workloads can be promoted (i.e., rehydrated) to VMware Cloud on AWS hosts after initial power-on of failover VMs, using optional Pilot Light clusters to make the recovery time even faster. VMs are maintained in their native vSphere format, which eliminates the need for brittle and time-consuming VM disk format conversions. Instant power-on of VMs is very powerful for rapid identification of the best recovery point when helping customers recover from a ransomware attack.

Easy-to-Use

During transient events such as DR testing or failover, partners don't need to learn new operational processes and tools of cloud infrastructure. They can manage both the cloud DR site and production sites with vCenter and retain access to familiar vSphere constructs such as clusters, resource pools, data stores, virtual switches, and port groups following a failover. The SaaS-based management console simplifies DR maintenance operations, eliminating the burden of managing the DR software, and allows scaling of up to 1500 VMs across multiple SDDC clusters. Continuous DR health checks occur every 30 minutes, thereby increasing the confidence that the DR plan will work when needed. "Audit-ready" built-in, automated audit reports help meet the end customer's internal policies and regulatory compliance requirements. A sophisticated DR workflow engine allows users to create customized and flexible recovery plans for hundreds to thousands of workloads. The Scale-out Cloud Filesystem checks the integrity of the data every day to confirm that the backup data is ready and usable when needed.

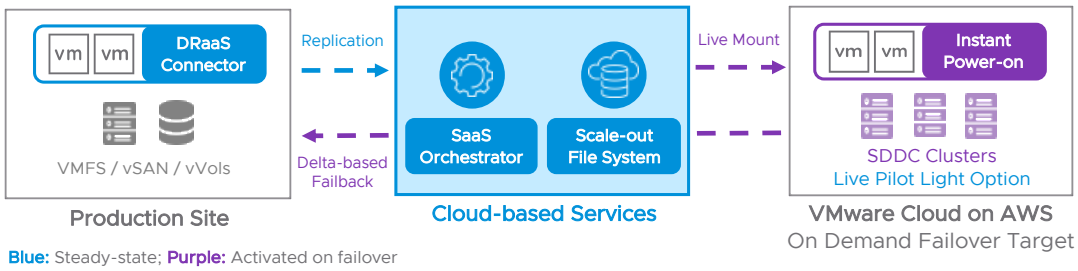

FIGURE 2: Steady-state Protection and Failover Conceptual Diagram

Cloud Economics

Leveraging the elasticity of cloud computing, VMware Cloud Disaster Recovery spins up VMware Cloud on AWS infrastructure only during a DR testing or failover event. It utilizes a highly efficient cloud storage layer for storing backups, which lowers the costs of DR. With a simplified pricing metric, customers pay for the DR service based on how much data is being protected[3] . Failbacks result in minimal AWS egress charges because only data deltas/changes are transferred.

VMware Cloud Disaster Recovery Use Cases

With VMware Cloud Disaster Recovery, partners can offer the ideal combination of cost-efficient cloud storage with simple SaaS-based management for IT resiliency at scale and a 'pay-as-you-go' failover capacity model — all with consistent VMware operations across production and DR sites. Below are the main use cases for VMware Cloud Disaster Recovery:

Recover from Ransomware: Non-disruptive validations of immutable cloud-based recovery points ranging from hours to months old and instant power-on of VMs in the cloud drive confidence in rapid ransomware recovery. However, some of these processes will still require some level of manual intervention. For enhanced, automated ransomware recovery capabilities, including guided restore point selection and Next-Gen AV and behavioral analysis embedded into a dedicated ransomware recovery workflow, use VMware Ransomware Recovery for VMware Cloud DR to accelerate recovery times, validate recovery points and prevent reinfection. *Learn more about VMware Ransomware Recovery*.

Expand or Replace Existing DR Site: Modernized DR operations delivered as a cloud-based service remove the need to own, rent or maintain secondary DR sites while reducing burden on IT teams and driving TCO reductions compared to traditional DR.

Optimize DR Costs: Many organizations overspend in backup and recovery, with VMware Cloud Disaster Recovery you can optimize you TCO by tuning your SLAs and costs to match application requirements, so you pay only for the protection you need—all within a familiar VMware ecosystem.

Audit-Ready DR: Automated health checks and workflows along with integrated reporting of testing, failover and failback operations drives compliance risk mitigation and provides proof that DR plans are being tested and executed correctly.

Remote Office/ Branch Office (ROBO) DR: Run business applications for up to 20 remote sites to restore apps in the event of a disaster and manage DR via a centralized SaaS-based management console.

[3] VMware Cloud on AWS SDDC capacity for testing and failover is paid for separately.
[4] Cybersecurity Ventures

Benefits for Partners and End Customers

HOW DO PARTNERS BENEFIT	HOW DO END CUSTOMERS BENEFIT
Partners don't need to re-train their entire IT team on a new, unfamiliar solution.	Customers can save their hardware dollars—it's all in the cloud.
Partners can test and orchestrate their customer's DR plans non-disruptively to drive DR readiness.	Customers can optimize DR costs and resource inefficiencies by tuning SLAs to match application requirements. They don't need to overspend on high availability for Tier 2 and 3 applications—they can simply choose between deployment models: fully on-demand for lowest TCO, and Pilot Light Mode for fastest recovery.
Partners can offer end-to-end VMware DRaaS with tightly integrated source vCenters and VMware Cloud on AWS with fast recovery 30-minute RPOs and up to *60% lower TCO* than traditional DR.	Customers can map RPO and RTO requirements and align them with their recovery strategies with defined criticality tiers. They can also customize their DR plans with ease of use and flexibility to match their business requirements with resource allocation efficiency.
Partners can leverage VMware investment by utilizing existing VMware training, operational models and tools as well as consistent operational environment across production and DR sites, offering DRaaS as a 100% SaaS agentless solution.	Customers can leverage cloud economics with a 'pay when they need' failover capacity model and benefit from no upfront application compute costs.

Helping Customers Create a Strategy

Before helping customers embark on their disaster recovery journey, partners can help them assess their existing environment, conduct a Business Impact Analysis (BIA), and map business demands to determine the best approach. They can ask them the below questions to gauge their needs:

- What do customers need to protect?
- How are they currently mitigating the risks associated with outages, availability, and other disruptions?
- What impact will DR have on their internal and external services?
- What are their compliance and audit requirements?
- What is their ransomware recovery strategy?

Once they've answered these questions, there's a final one that often goes overlooked:

Can they reliably conduct DR operations while tuning their level of protection to match their Service Level Agreements (SLAs)? More specifically, can they find an optimized balance between reliable protection and efficient allocation of DR resources? With VMware Cloud Disaster Recovery, they will be able to.

Partners can help customers be DR ready in 5 easy steps. They can help customers understand how quickly and easily they can protect their on-prem data center site(s) with VMware Cloud on AWS.

Once the solution is procured and ready to deploy, DR administrators can follow a similar set of tasks to get their organization ready for failover to the cloud in short order:

- Day 1: Planning
  - **Map Applications**: Determine the VMs to be protected by VMware Cloud Disaster Recovery and organize them into preliminary application DR sets for protection policy assignment and DR plan step(s) processing
  - **Align SLAs**: Align available SLAs and initial retention objectives that are to be applied after initial snapshot copy to the cloud
  - **Organize On-Prem Resources**: Define and document the on-prem organization of compute resources, folders, networks, and tags that may be used to identify and place VMs in the SDDC
- Day 2: Define
  - **Build Site**: Construct the protected site(s) that contain the target VMs – includes up to 6 DRaaS Connectors and 2-3 vCenters
  - **Define Policies**: Construct a test protection group for a small sample VM set for each protected site to verify prem-cloud operations
  - **Configure**: Construct initial protection group policies for the VMs defined in the application DR sets on Day 1 (set inactive for this phase) – includes up to 10 policies
  - **Begin Data Copy**: Take manual snapshots of protection groups – use relative prioritization and/or data set size to optimize initial transfer readiness
- Day 3: Configure
  - **Deploy Cloud Site**: Deploy the VMware Cloud SDDC test site – use a 1-host footprint to minimize costs and familiarize with the process
  - **Align Sites**: Modify the SDDC to the desired configuration to align with on-prem site(s) – includes resource groups, folders, networks, tags, and test bubbles setup
  - **Define DR plans**: Define DR plans using the application organization details from Day 1
- Day 4: Test
  - **Test Failovers**: Begin DR plan failover testing – using the NFS datastore for initial steps alignment
  - **Measure Results**: Run a DR plan test with full SDDC migration (Storage vMotion) to understand operational results – pick a smaller application data set (less than 1TB)
  - **Adjust Plans**: Adjust DR plans based on any performance or sizing findings in the testing processes
- Day 5: Operate
  - **Review Runbooks**: Review reports for compliance and plan details and review runbooks for test runs from Day 4
  - **Monitor Sites**: Monitor progress of on-prem site protection and compliance checking
  - **Report and Audit**: Document and remove the test SDDC

It's just as easy to maintain this setup with revisions and repeating the steps as new workloads are included .

There are some assumptions made for this 5-day scenario:

- Assuming a 1 Gbps link to AWS provides about 10TB/day data rate to enable up to ~20 TB to protect in 2-3 days to enable protection of VMs to be tested
- Does not include major site overhaul to run applications in a hybrid cloud environment. That is more NSX/ HCX/ VMC/ AWS related and outside the scope of this proposal
- Assumes network connectivity from prem-cloud has been established and team has all of the necessary privileges and access needed to perform tasks
- Does not include core infrastructure modification to support hybrid or cloud only operations (e.g., DNS, DHCP, load balancing, VPN, firewalls, etc.)
- Does not include DR plan Script VM customizations – a sample script VM can be included in the prepare and test phases as example only

MSP Platform

The Managed Service Provider (MSP) route to market gives partners the option to use VMware Software-as-a-Service offerings without investment in their own data center infrastructure, delivering managed services on top. VMware Cloud Disaster Recovery will be offered to our MSPs through our centralized service provisioning portal, the VMware Cloud Partner Navigator which helps MSPs transact, deploy, and provision SaaS offerings from a single pane of glass.

How to Get Started

Below is an overview of the VMware Managed Service Provider (MSP) lifecycle:

Commit Contract – Partner signs a VMware Cloud Disaster Recovery Managed Service Provider commit contract with a VMware Aggregator. Partner then commits to VMware an MSRP (list price) spend to obtain a volume discount for their purchases.

Cloud Provider builds MSP Pipeline – Partner initiates go to market activities and starts building their business for Managed Services.

Deliver Managed Services and Own the Terms of Service – Once the opportunity has been identified, partners can order VMware Cloud Disaster Recovery from VMware and provide managed services as part of the offering to their customers. Partners must provide their own terms of service and managed services as part of the offering to the end customer. At a minimum, this must include technical support for the service and all functions associated with service configuration, add-ons, renewals and anything pertaining to billing.

On-Board and Provide Support to their Customers – Partner will on-board VMware Cloud Disaster Recovery for their customers. Subsequently, they may obtain technical support from VMware as needed, with the following *provisions*. In turn, partners are responsible for all customer support, which may include but may not be limited to customer communication, any managed services, answering installation, configuration, and usage questions.

Complete Monthly End Customer Reports and Pay Invoices – On the 10th of every month, the partner will log into the VMware Commerce Portal and review the prior month's usage. Partner will review the report and submit it to their Aggregator by the 15th day of the month. Following that, the Aggregator will send the partner an invoice for the month.

Access the MSP end-to-end getting started guide *here*.