Technology Guide

Disaster Double Trouble

A unified methodology for addressing the unique challenges of disaster recovery (DR) and ransomware recovery

vmware®

Business interruptions and losses from disasters and ransomware are on the rise. By 2031, it's expected there will be a cyberattack every two seconds.[1]

Double-up your defenses

With the best practices, techniques and solutions mentioned in this guide, your organization will be positioned to:

- Unify your DR and ransomware recovery management.
- Level up your recovery capabilities.
- Reduce total cost of ownership (TCO) by up to 60 percent compared to on-premises DR.
- Simplify operations, upgrades and maintenance.
- Align recovery point objectives (RPOs) and recovery time objectives (RTOs) with the needs of your business.

Whether critical data and operations loss are caused by a wildfire or a ransom-seeking cyberattacker, the result is the same: Business continuity (BC) crashes to a halt and financial damages mount, with data breaches costing an average of $4.35 million in 2022, according to IBM Security.[2] Because of their similar negative outcomes, disaster recovery (DR) and ransomware recovery are commonly lumped under a one-size-fits-all disaster management strategy by organizations. However, that's not the best approach.

While you should assess both general DR and ransomware recovery needs together for the greatest efficiency and resiliency, failing to recognize the unique challenges and considerations of each type of threat is a recipe for disaster.

This guide is designed to serve as a starting point for aligning these two strategies.

Two types of threats. Two solutions to integrate.

	On-Demand Disaster Recovery	Next-Gen Ransomware Recovery
Nature of threat	One-time natural disaster, human error, or equipment failure event	Sophisticated, malicious, covert, ongoing attacks
Solution requirement	Rapid restoration of business operations at scale	Rapid recovery without reinfection, detection of next-gen ransomware

1 Cybersecurity Ventures. "Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031." July 7, 2023.
2 IBM Security. "Cost of a Data Breach Report 2022." July 2022.

Rapid recovery techniques

Time is of the essence when it comes to ensuring business continuity. The following techniques, which are included in VMware Cloud Disaster Recovery™ and VMware Ransomware Recovery™, enable rapid recovery from a variety of disaster scenarios.

Point-in-Time Recovery

Ideal for accidental data deletion

Restoring to an exact point in time enables you to rewind to just before a disaster or data corruption occurred. This is helpful if you know exactly when the problem truly began.

Failover Mechanisms

Ideal for hardware failures and planned shutdowns

When a primary system fails, failover mechanisms automatically switch and redirect requests to a secondary system that mimics the primary system's environment.

Seven steps to develop a "double trouble" recovery plan

A robust disaster and ransomware recovery planning process identifies what to protect and how to protect it. Here are the steps to take:

1. **Assess:** Inspect, catalog and map your data estate. Determine what protection your workloads and virtual machines need. Think about how you can optimize resources to support both recovery operations without compromising reliability.

2. **Define:** Outline the scope of both recovery plans, including your goals (RTOs and RPOs), SLAs, protection schedules and length of storage. Consider including the two rapid recovery techniques outlined on this page.

3. **Procure:** Obtain and integrate the solutions, vendors, storage and assets you need to achieve your newly outlined plans. You might want to include a managed solution for disaster recovery as a service (DRaaS) and ransomware recovery as a service (RRaaS) to help you.

4. **Build and replicate:** Build recovery sites, create protection groups, and replicate your data using secure mechanisms and storage.

5. **Configure:** Build out failover plans, test them, and align your sites. Create an isolated network to support quarantine, testing and validation of snapshots in case ransomware strikes.

6. **Test:** Test your recovery plans regularly to ensure they are nondisruptive and ready for a real-world incident. Continuously adjust and iterate based on the test results.

7. **Operate:** Ensure your protection groups are running, check your overall recovery conditions, run reports, and compare results against your expectations and SLAs.

Don't forget to take all potential disaster and ransomware scenarios into account as you work through each of these steps. Doing so will set you up for a rapid, successful recovery, no matter what fate sends your way.

The benefits of managed DRaaS and RRaaS

Daunted by the complex management requirements of recovery? Think that it comes at a high cost? Worried about the reliability of your solutions or processes? Put your mind at ease with the right managed DRaaS and RRaaS solutions for your organization.

Reliability at scale

With a high-confidence managed recovery solution, your organization can preserve data availability at scale and rapidly recover your mission-critical workloads.

Reduced costs

By using cost-efficient cloud storage and paying only for failover capacity when needed, you eliminate the need for a secondary data center and specialized recovery assets.

Simplified operations

With managed DRaaS and RRaaS, you can easily define, maintain and test failover procedures in a constantly changing IT environment—and rapidly spin up failover capacity when a disaster occurs.

Rapid ransomware recovery

Minimize downtime and data loss in the face of ransomware threats through guided automation and safe recovery with integrated availability, security and networking.

By leveraging a DRaaS or RRaaS partner's wealth of expertise, you can implement a robust plan in less time and avoid costly, irreparable mistakes. These partners might even help create and implement an end-to-end protection and recovery strategy that meets your recovery needs and leverages native integrations, so you can seamlessly recover with agility.

Real stories of resilience

See how two organizations boost their resiliency with VMware.

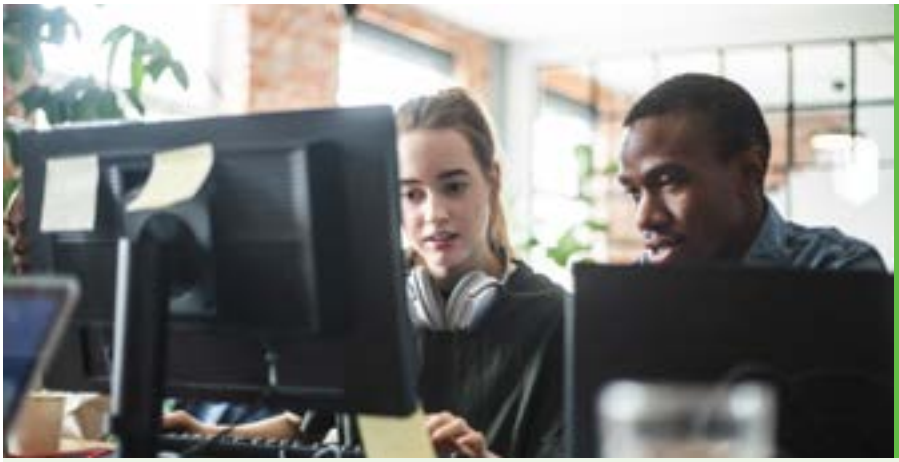
"After implementing VMware Cloud Disaster Recovery, I certainly sleep much better."

—Ivan Slavioglo, Vice President of IT, Fozzy Group

Fozzy Group protects IT operations in a war zone

Leading Ukrainian retailer Fozzy Group's leaders needed to be confident that their essential infrastructure would be available despite wartime attacks, including ransomware. Fozzy previously used a variety of loosely coupled systems, resulting in a difficult-to-test recovery plan. Now, VMware Cloud Disaster Recovery helps ensure that Fozzy Group can continue to supply essential goods for its customers.

Read the Case Study



"VMware Cloud Disaster Recovery just works. I don't lose sleep over our ransomware recovery capability."

—Greg Morrissey, IT Manager, Merrick and Company

Merrick protects their digital assets from ransomware

Merrick cut their costs and reduced their recovery time from days to minutes with VMware Cloud Disaster Recovery. Before, they used a complex, costly web of components and rented data centers to serve as protection from disaster. Merrick now uses VMware Cloud Disaster Recovery for ransomware and disaster protection, which integrates with existing VMware infrastructure, and uses the cloud as a failover target.

Read the Case Study

Explore supercharged, cloud-powered recovery

VMware Cloud Disaster Recovery and VMware Ransomware Recovery can be consumed right from your VMware vSphere+™ cloud console. This solution facilitates a surprisingly smooth transition from manual, multi-vendor, expensive on-premises DR to unified, resilient, automated cloud operations with confident recovery.

Protect your data in all locations with a single cloud-based solution for disaster and ransomware recovery—one that includes a dedicated ransomware recovery workflow that integrates capabilities to identify, validate and restore workloads at scale. Prevent reinfection using a push-button, fully managed isolated recovery environment (IRE) to test and iterate. Provision failover capacity only when you need it, directly from your VMware Cloud Disaster Recovery console, with an IRE to prevent reinfection of production workloads, embedded next-generation antivirus and behavioral analysis, and guided restore point selection.

These highly scalable, on-demand VMware-managed services enable organizations to:

- Get to value in a matter of hours.
- Deploy, manage and test with automation.
- Save on hardware, maintenance and labor.
- Shrink CapEx and achieve up to 60 percent lower TCO compared to traditional DR.

Still on VMware vSphere? Upgrade to VMware vSphere+ before adopting DRaaS.

Build on your existing investments. Upgrade to VMware vSphere+ and easily extend your on-premises IT infrastructure to the public cloud while leveraging existing skills, tools and processes.

Consume services and capabilities through your VMware vSphere+ cloud console, including HCI, DRaaS, ransomware protection, enterprise app infrastructure as a service (IaaS), automation, developer services and more. Take advantage of cloud management and economics without disrupting your current infrastructure or operations.

VMware vSphere+ supercharges performance, enhances operational efficiency, and accelerates innovation.

Start Your Upgrade