VMware Ransomware Recovery

An end-to-end, integrated easy-to-use solution that accelerates ransomware recovery with minimal data loss using an on-demand isolated recovery environment

What is VMware Ransomware Recovery for VMware Cloud DR?

A purpose-built ransomware recovery-as-a-service solution that:

- Identifies recovery point candidates
- Validates restore points
- Prevents reinfection
- Minimizes downtime and data loss

Ransomware is here to stay – Cybersecurity Ventures estimates a ransomware attack occurs every 11 seconds and costs victims billions in damages worldwide. To combat, the National Institute of Standards and Technology (NIST) recommends implementing a robust ransomware protection plan that includes both preventative and recovery measures.

When considering a disaster recovery or backup solution, organizations need to look for one that understands how ransomware operates and can mitigate the unique risks it poses. Because ransomware can dwell, often remaining undetected for weeks or even months, when an organization is attacked, it has to be assumed the primary datasets and backup copies may already have been infected. This means organizations need a way to quickly test their backups to find those that have not been infected to support a clean restore. Unfortunately, since most ransomware attacks today involve fileless techniques, recovery solutions designed for ransomware recovery have to go beyond traditional file scanning to adequately validate restore points and prevent reinfection. This is what VMware offers.

VMware Ransomware Recovery for VMware Cloud Disaster Recovery™ has been purpose-built for ransomware recovery. It offers accelerated ransomware recovery with minimal data loss, delivered as an end-to-end, integrated, and easy-to-use SaaS solution. It is a purpose-built ransomware recovery-as-a-service solution, enabling safe recovery that prevents reinfection of production workloads using an isolated recovery environment in the cloud. Guided recovery workflows allow organizations to quickly identify recovery point candidates, validate restore points using embedded behavioral analysis, and recover data with minimal loss, so they can quickly get back to business.

VMware Ransomware Recovery overview

VMware Ransomware Recovery is a purpose-built, industry-leading ransomware recovery-as-a-service solution that empowers organizations to recover from ransomware attacks with confidence and agility. Organizations benefit from a dedicated ransomware recovery workflow that has deeply integrated recovery automation capabilities including an on-demand Isolated Recovery Environment (IRE) to prevent re-infection of production workloads, guided restore point selection, and embedded next-generation antivirus and behavioral analysis.

Why VMware Ransomware Recovery?

To combat the rising threat of ransomware, VMware Ransomware Recovery provides a purpose-built solution that:

- Accelerates recovery times
- Protects the integrity of an organization's data
- Simplifies operations with an easy-to-use end-to-end solution

VMware Ransomware Recovery builds upon the rich set of foundational capabilities that VMware Cloud Disaster Recovery already provides for rapid ransomware recovery. These include deep snapshot history, high-frequency snapshots, immutable snapshots that are stored in an operationally air-gapped environment, instant virtual machine (VM) power-on for rapid experimentation, daily data integrity checks, and file- and folder-level restore—all as a managed service, and at a low total cost of ownership.

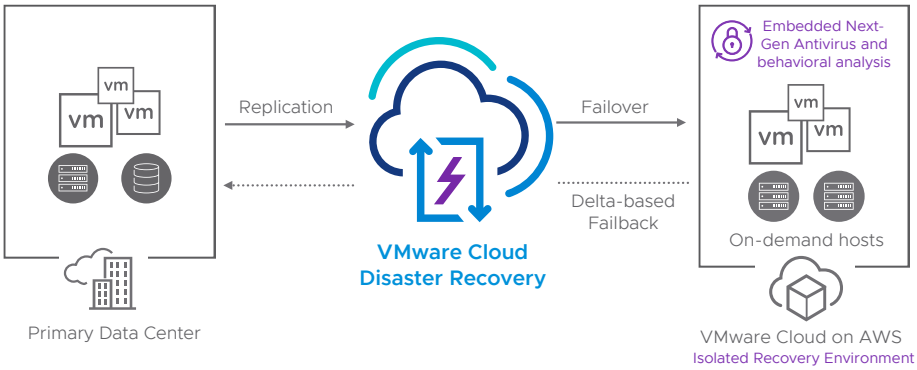

Figure 1: VMware Ransomware Recovery.

VMware Ransomware Recovery benefits

Accelerated recovery times

With a dedicated ransomware recovery workflow that integrates automated recovery point identification, validation, and restore to get organizations back up and running fast. Rapid recovery point iterations allow organizations to quickly find clean restore points and data across multiple backup copies through an iterative process. Zero copy and no rehydration of data from cloud storage to VMware Cloud™ on AWS hosts (Instant power-on from Live Mount of NFS onto SDDC clusters) makes restoration fast. Instant power-on is very powerful for rapidly identifying which recovery point to restore. Organizations can take advantage of push-button VM network isolation levels within the guided workflow to isolate VMs from one another to prevent lateral movement of ransomware. They can also create custom isolation rules. With file- and folder-level recovery, recovery points can be analyzed individually to extract uncompromised data and merge it into a final recovery point, thus minimizing data loss and time to recovery.

Data integrity

Data integrity is preserved with an on-demand Isolated Recovery Environment (IRE) that can be used to stage candidate recovery points and prevent reinfection of workloads. Protected workloads and data are forever incremental, encrypted, and stored in redundant cloud storage. Immutable snapshots are stored in a secure, operationally air-gapped Scale Out Cloud File System (SCFS), preserving data integrity at the time of recovery. The SCFS checks the integrity of the data every day to confirm that the

backup data is ready and usable when needed. Automatic health checks of the recovery plan every 30 minutes increase the confidence that the recovery plan will work when it's time to failover. Role-based access control allows organizations to tightly restrict and audit permissions. They also have access to the history (hours, days, weeks, months) of snapshots – which can be done as often as every 30 minutes – per VM (up to 2000 snapshots per protection group) to ensure nothing is missed.

Simplified operations with an easy-to-use end-to-end solution

Organizations don't need to learn new operational processes or cloud tools to use VMware Ransomware Recovery. The entire ransomware recovery process can be managed through VMware vCenter®, a SaaS-based management console. Deeply integrated recovery automation capabilities within the ransomware recovery workflow delivered through a simple, clickthrough experience further accelerate recovery. Built-in failback capabilities efficiently orchestrate a failback from VMware Cloud on AWS to the original production site. Ransomware recovery support for up to 6000 VMs with the ability to spin up many SDDC clusters allows organizations to scale to easily protect entire datacenters.

VMware Ransomware Recovery use cases

Rapidly identify good recovery point candidates

Ransomware can remain undetected and propagate for a long time. As a result, to find a recovery point that hasn't been compromised, organizations may have to look deep into their backup catalogs – they could have to look at thousands of restore points. It can be difficult to even know where to start, and most don't have the tools or insights to be able to quickly determine which recovery point candidates are good.

VMware's guided restore point selection presents insights such as VMDK rate of change and file entropy in a single view along with the snapshot timeline to help organizations locate good recovery point candidates fast.

Validate good restore points

Once an organization has identified good recovery point candidates, they must validate they are free of malware. Most attacks today involve fileless techniques, which cannot be detected with traditional file scanning. This means organizations need to be able to run next-generation antivirus and behavioral analysis on powered-on workloads to properly validate restore points.

VMware's embedded recovery point scanning applies a variety of techniques, including signature-based scanning, vulnerability assessment, and behavioral analysis, to validate snapshots. With rapid recovery point iterations, organizations can quickly find clean restore points and data across multiple backup copies.

Prevent reinfection

It is important to prevent reinfection in a ransomware recovery operation. This requires an environment that can properly isolate workloads and prevent lateral movement if a compromised snapshot is restored, which can be difficult to set up, manage, and maintain. It also requires the organization to set up network isolation policies for VMs. These often have to be manually configured, which can be a burden on IT and thus increase the chance of error (and reinfection).

VMware offers a managed, on-demand Isolated Recovery Environment (IRE) that takes the burden off of organizations and provides an additional layer of security. Immutable snapshots are stored in a secure, operationally air-gapped Scale Out Cloud File System, to preserve the data integrity at the time of recovery. In addition, organizations can take advantage of VMware's push-button VM network isolation levels within a guided workflow to easily isolate VMs. They can also create custom isolation rules if needed.

Limit data loss

The farther an organization goes back in time within a snapshot to select the restore point, the lower the risk of infection, but the higher the risk of data loss. To limit data loss, organizations need a better way to rapidly find unencrypted files and data among many recovery points and use fine-grained recovery techniques.

VMware provides file- and folder-level recovery that allows recovery points to be analyzed individually and uncompromised data extracted and merged into a final recovery point to minimize any data loss while speeding time to recovery.

Efficiently recover from ransomware

Many organizations need to leverage multiple DR and security tools to try to recover from a ransomware attack. Standard DR solutions are designed with disaster recovery in mind – they are optimized to orchestrate a mass data center recovery using the most recent recovery point, which may not be appropriate (or safe) when dealing with a ransomware attack. Many DR products lack the dedicated, iterative workflows needed to aid in efficient ransomware recovery.

VMware provides an end-to-end, easy-to-use automated ransomware recovery workflow that simplifies and accelerates the entire process. Rapid recovery point iterations quickly find clean restore points and data across multiple backup copies to optimize the recovery. In addition, built-in failback capabilities mean organizations don't have to take this important step on their own. As a SaaS offering, there is nothing for the organization to build, install, or maintain.

Let's get started

VMware Ransomware Recovery delivers safe, controlled recovery after a ransomware attack to help organizations return to business as usual as fast as possible. Visit these sites to learn more:

VMware Ransomware Recovery

VMware Cloud Disaster Recovery

VMware Ransomware Recovery supports Multi-Cloud and Intrinsic Security

Planning for the worst is a critical element of any organization's multi-cloud strategy. VMware Ransomware Recovery is an extension of VMware's overall Disaster Recovery portfolio, providing on-demand ransomware recovery-as-a-service for vSphere workloads running on-premises or in VMware Cloud on AWS. The addition of VMware Ransomware Recovery gives organizations a platform for protecting their enterprise applications and data.

Within Intrinsic Security, VMware Ransomware Recovery offers a comprehensive ransomware protection solution that is built into the virtualization layer across the entire ransomware protection cycle: Identify, Protect, Detect, Respond and Recover. VMware Carbon Black® and VMware NSX® Advanced Firewall address the initial stages of this ransomware protection cycle, while VMware Ransomware Recovery provides the last line of defense and leverages native integrations with these security products, so they work better together. Furthermore, VMware Professional Services can help create and implement an end-to-end ransomware protection and recovery strategy to meet the organization's specific needs.

Item No: VMware Ransomware Recovery Solution Overview 10/22