Well-Architected Design: VMware Cloud Ransomware Recovery

Table of contents

Well-Architected Design: VMware Cloud Ransomware Recovery 3

Introduction 3

Scope of the Document 3

Summary and Considerations 4

Background 5

Ransomware Recovery Planning 6

Phases Ransomware Recovery Planning 6

Preparation and Dwell Time 7

Replication 7

Longer Snapshot History 7

Isolated Recovery Environment 7

Network Isolation 7

Guided Restore Point Selection 7

Change Rate and Entropy 8

Ransomware Recovery Flow 8

Ransomware Recovery Process 9

Snapshot Selection 10

Operating System Validation 11

Fine Tuning 11

Staging and Recovery 11

Conclusion 11

Well-Architected Design: VMware Cloud Ransomware Recovery

Introduction

VMware Cloud Disaster Recovery offers a comprehensive solution for ransomware recovery, providing organizations with the tools and capabilities to mitigate the impact of ransomware attacks and quickly restore their critical systems and data. Ransomware is a type of malicious software that encrypts files and demands a ransom payment in exchange for the decryption key. VCDR's ransomware recovery features help organizations protect their data, detect ransomware attacks, and recover from such incidents efficiently.

Scope of the Document

The purpose of the Ransomware Recovery Document is to provide a clear roadmap and plan actionable steps for organizations to recover their systems, data, and operations in the aftermath of a ransomware attack. It serves as a reference guide for incident response teams, IT administrators, and other relevant personnel involved in the recovery process.

Summary and Considerations

Use Case	
Pre-requisites	
General Considerations/Recommendations	
Performance Considerations	
Network Considerations/Recommendations	network isolation
Last Updated	Oct 2023

Background

Ransomware Recovery and Disaster Recovery are two distinct concepts, but they are related and complement each other in an organization's overall cybersecurity strategy. Let's compare these two processes:

Ransomware Recovery	Ransomware recovery specifically deals with the process of recovering from a ransomware attack. It involves restoring data, systems, and services that have been encrypted or compromised by ransomware.
Disaster Recovery	Disaster recovery refers to a broader set of strategies and procedures for recovering from any type of disaster or disruptive event, such as natural disasters, hardware failures, cyberattacks, or human errors. It encompasses a wide range of recovery efforts to resume business operations after such incidents.

VMware Ransomware Recovery (RWR) is available as an addon on VMware Cloud Disaster Recovery to help organizations protect their data, detect ransomware attacks, and recover from such incidents efficiently. With VMware Cloud Disaster Recovery, organizations can create recovery plans specifically designed for ransomware recovery. These plans include integrated security and vulnerability analysis, behavioral analysis, and malware signature scanning to detect and mitigate ransomware threats.

In the event of a ransomware attack, VMware Cloud Disaster Recovery enables organizations to activate recovery plans, triggering the recovery process. The ransomware-infected systems can be isolated, and clean snapshots or backups can be restored to restore the affected systems to a known good state. VMware Cloud Disaster Recovery provides options to recover individual virtual machines or entire groups of machines, allowing organizations to tailor their recovery strategy based on the scope of the attack.

Furthermore, VMware Cloud Disaster Recovery offers features like granular file-level recovery, which enables the recovery of specific files or folders that may have been encrypted by ransomware. This allows organizations to restore only the necessary data, minimizing downtime and reducing the impact of the attack.

Ransomware Recovery Planning

There are many planning and deployment considerations when implementing a VMware Cloud ransomware recovery environment, there are many considerations. While VMware's Ransomware Recovery solution provides an extensive set of capabilities to assist in workload recovery following a ransomware attack, it requires an understanding of the basic structure of common ransomware attacks to chart an optimal path to recovery.

The National Institute of Standards and Technology (NIST) defines a 5-phase Ransomware Recovery Framework.

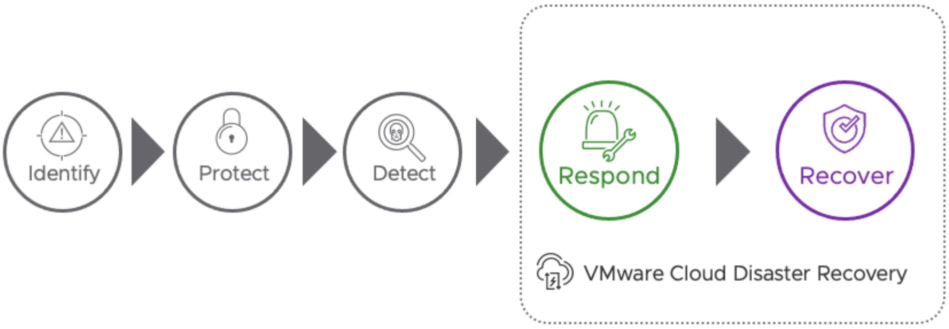

Figure 1 – NIST Framework

VMware Ransomware Recovery focuses on the Respond and Recover phases of the framework: it is the last line of defense in case your protections have been bypassed and detection has perhaps come too late to for prevention. While corporate security and risk teams typically manage the left side of the NIST framework, it almost always falls on the IT infrastructure team to manage response and recovery tasks as such use of tools that streamline otherwise manual recoveries is critical for speed and success.

The Design Planning for Ransomware Recovery covers the following key areas:

Backup and Recovery Strategy	Guidance on designing a robust backup and recovery strategy that ensures regular and secure backups of critical systems and data, considering factors such as backup frequency, retention periods, and offsite storage.
Security Measures	Recommendations for implementing security controls to prevent ransomware attacks, including endpoint protection, email security, network segmentation, and user awareness training.
Incident Response Planning	Guidelines for developing an effective incident response plan that includes clear roles and responsibilities, incident detection and reporting mechanisms, and containment and recovery procedures.
Recovery Infrastructure	Considerations for designing the recovery infrastructure, such as the selection of recovery sites, network connectivity, scalability, and redundancy.
Data Integrity and Validation	Best practices for ensuring the integrity and authenticity of recovered data, including data validation processes, encryption, and secure transmission.
Testing and Maintenance	Recommendations for conducting regular testing and maintenance of the ransomware recovery solution, including simulated recovery exercises and updates to reflect changing threats and technologies.
Compliance and Regulatory Requirements	Guidance on aligning the ransomware recovery solution with applicable industry regulations and compliance standards.

Phases Ransomware Recovery Planning

Preparation and Dwell Time

Preparation is critical to successful recovery from a ransomware attack. Ransomware poses a unique challenge due to a concept known as *dwell time.* Ransomware dwell time refers to the duration of time between when a ransomware attack initially breaches a system and when it is detected by the victim organization. During this time, attackers can move laterally within the network, escalating their privileges, gathering sensitive data, or establishing persistent access to compromised systems.

Replication

Replication for ransomware recovery follows the same guidelines as for VMware Cloud Disaster Recovery regarding the amount of data, number of virtual machines, clusters, vCenter servers, DRaaS connectors, bandwidth, etc. Most actions during ransomware recovery are performed on individual virtual machines, so the protection groups are primarily used to ensure that snapshot schedules and retention configurations match the business continuity requirements of the organization. It is typical for the same protection groups to be used for VMware Cloud Disaster Recovery as for Ransomware Recovery, just with expanded snapshot lifetimes.

Longer Snapshot History

For traditional disaster recovery, having snapshots going back a month or even a couple of weeks may be sufficient. In fact, most DR events use the latest snapshot for recovery. However, due to the likely long-dwell time of undetected ransomware, common analyst guidance suggests maintaining recoverable backups for at least 3 months and often 6 months. This will increase the amount of storage consumed in your cloud file system and therefore will impact cost considerations.

Isolated Recovery Environment

The generally accepted industry definition of an Isolated Recovery Environment (IRE) typically refers to a segregated network or system used exclusively to run workloads during ransomware recovery. This environment and its networking are physically or logically separated from the production network to prevent the spread of ransomware while suspect workloads are brought online and analyzed. An IRE utilizes independent infrastructure with access to secure backups of critical data and systems. Access to an IRE is limited to authorized personnel and typically have strong authentication measures in place.

VMware Cloud Disaster Recovery Ransomware Recovery leverages a VMware Cloud on AWS Software-Defined Datacenter (SDDC) as a recovery site, which is then enabled as an IRE by using the functionality of VMware NSX Advanced Firewall to effectively deploy a per-VM IRE, so each VM is securely recovered in total isolation, even from other VMs on the same network.

Network Isolation

Enabling this option incurs a small incremental per-host cost in the recovery SDDC, but only when a ransomware recovery plan is activated and in progress. While it is possible to leverage NSX capabilities without turning on NSX advanced firewall, this feature provides significant additional security and network quarantine options. It is highly recommended to help prevent the lateral spread of malware between virtual machines on the segment and allow for granular behavioral analysis at different phases of the recovery process.

The impact of this feature can be easily seen by the availability of additional options on the Network Isolation configuration of a virtual machine when performing a ransomware recovery or test. These isolation options can limit access to virtual machines on the internal network, as well as provide a Quarantined + Analysis option that permits the VMware Carbon Black sensor to be installed, and its behavioral analysis data to be uploaded to the VMware Carbon Black cloud while not permitting general access to the Internet.

Guided Restore Point Selection

For recovery plans actively going through ransomware recovery, the Guided Restore Point Selection feature assists in the location of uncompromised snapshots. Using a measured rate of change and entropy between adjacent snapshots, administrators can identify snapshots that have experienced a great deal of data change and large-scale encryption events, and then select a snapshot prior to these events as a recovery candidate.

During the recovery process, snapshots can be badged after review to easily identify their state. Snapshots can be identified as being clean, having concerns, malware being present, or being encrypted. This process is manual, as snapshots will default to having no badge. Once a snapshot has been badged, the badge will show up in the Guided Restore Point timeline to facilitate further snapshot selection activities.

Badge	Comment / Use
Not badged (default)	No information on the security status of this snapshot.
Verified	This snapshot is safe.
Warning	Some of the data in this snapshot might be compromised, but overall infection is uncertain.
Compromised	Vulnerabilities and malware infections were found on the VM snapshot.
Encrypted	Data in this snapshot is encrypted by ransomware.

Change Rate and Entropy

Based on common actions performed by current malware, change rate and entropy are indicators of malware activity. Understanding how these metrics can be used to locate points of potential malware execution is best conveyed through an example. Spikes in either of these two graphs may signify that malware has begun deleting or encrypting data within the virtual machine. This information, presented in a pair of histograms can quickly guide the selection of points in time when such activities have occurred and enable recovery from the nearest snapshot prior to the malicious activity.

Ransomware Recovery Flow

The recovery process flow can be seen in the following diagram. During each step in the recovery process, indications of compromise should be checked while evaluating the risk of the current iteration against the speed of recovery.

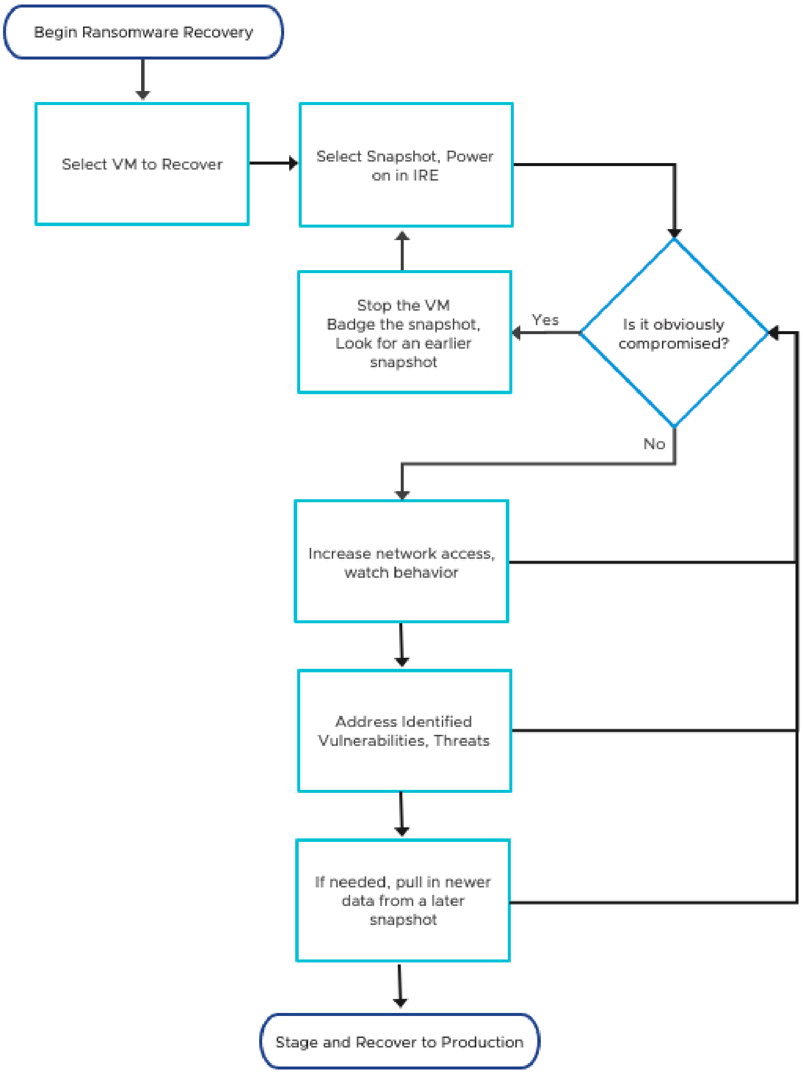
Begin Ransomware Recovery
Select VM to Recover
Select Snapshot, Power on in IRE
Is it obviously compromised?
Yes
Stop the VM Badge the snapshot, Look for an earlier snapshot
No
Increase network access, watch behavior
Address Identified Vulnerabilities, Threats
If needed, pull in newer data from a later snapshot
Stage and Recover to Production

Figure 6 – A typical ransomware recovery flow

Ransomware Recovery Process

The process of recovering from a ransomware attack is significantly more complex than recovering from a traditional disaster:

- A typical disaster recovery process leverages orchestration to turn on VMs in a specific order, all from the same point in time, on a live running network intended to resume business operations.

- When ransomware attacks, it does not affect all VMs at the same point in time, so a per-VM workflow that allows recovery of all VMs from potentially different points in time becomes critical.

- When recovering from ransomware, starting all VMs on a live routed network with the assumption that business operations will resume is not advised, as unintentionally recovering infected workloads could result in re-infection of clean machines or, worst case, spread back to an already cleaned environment.

With the tools and workflows provided by VMware Cloud Disaster Recovery, recovery efforts can be better managed and return to service can be established much more quickly.

The ransomware recovery process involves the following phases:

Detection and Isolation	Identify the ransomware incident through monitoring systems, user reports, or security alerts. Isolate the affected systems or devices to prevent further spread of the ransomware.
Incident Response	Activate the incident response plan and assemble the response team. Notify relevant stakeholders, including IT, security, legal, and management teams. Gather evidence and document the details of the ransomware attack.
Recovery Plan Activation	Initiate the ransomware recovery plan, which includes predefined steps and procedures for recovering from the attack. Determine the scope of the recovery, such as the affected systems, data, and applications. Consider any regulatory or compliance requirements that may impact the recovery process. This is a iterative process until a clean copy of effected VM(s) is determined.
Data Restoration	Restore data from clean backups that were not affected by the ransomware attack. Verify the integrity and reliability of the restored data. Prioritize the restoration of critical systems and data to minimize downtime.
Infrastructure and System Rebuilding	Rebuild or restore the affected infrastructure components, including servers, networks, and endpoints. Apply necessary patches, updates, or security configurations to strengthen the security posture.
Malware Removal and Remediation	Perform thorough malware scans and removal processes on all affected systems. Update antivirus and anti-malware solutions with the latest definitions. Conduct security audits to identify vulnerabilities and implement appropriate security measures.
Security Enhancements	Strengthen security measures, such as implementing multi-factor authentication, access controls, and endpoint protection solutions. Improve security awareness training for employees to prevent future incidents.
Post-Recovery Testing and Validation	Conduct comprehensive testing and validation to ensure the effectiveness of the recovery process. Verify that critical systems and data are functioning as expected. Test incident response procedures to identify areas for improvement.
Lessons Learned and Documentation	Conduct a post-mortem analysis to identify the root cause of the ransomware attack and evaluate the response and recovery efforts. Document lessons learned, including recommended improvements to prevent future incidents. Update the incident response plan and ransomware recovery procedures based on the lessons learned.
Ongoing Monitoring and Maintenance	Implement continuous monitoring of systems and networks to detect any signs of ransomware or suspicious activity. Regularly review and update security measures to stay resilient against evolving ransomware threats. Conduct periodic security assessments and penetration testing to identify vulnerabilities.

The recovery process is iterative in nature, and it is important to set the expectation early on that this is not simply a “roll back to the latest snapshot and carry on” endeavor. If approached that way, the recovery may be quick, but the odds of reinfection or reactivation of an existing infection are very high. In addition to recovering to a snapshot that has yet to be affected by the malware, a true recovery requires scanning for the source of the infestation, removing it, and patching the machine to prevent future infections.

From a high level, this process can be broken down into four phases:

1. Snapshot Selection
2. Operating System Validation
3. Fine Tuning
4. Staging and Recovery

Snapshot Selection

In this phase, the goal is to locate the best point in time for a recovery baseline. This is a snapshot that is as current as possible while also being unaffected by malware detonation. The goal is to find something that can be cleaned of malware and patched to prevent the malware from impacting it. This is where the functionality of the Scale-out Cloud File System (SCFS) and the Guided

Restore Point Selection workflow are important. The ability to filter snapshots in the inventory by using data change characteristics, along with the ability to quickly iterate through the available snapshots enables significantly faster recovery, than restoring from tape or even online media servers.

The SCFS stores snapshots as full VMs, which can be instantly presented on a live NFS datastore which allows VM power on operations within 30-60 seconds regardless of whether the VM is 10GB, 100GB, 1TB or 20TB. This allows rapid iteration within the recovery SDDC without engaging a backup operations team or performing tedious backup restore processes.

Operating System Validation

Once a viable snapshot has been selected, this phase involves watching the behavior of the running virtual machine through use of the integrated Carbon Black solution for suspicious behavior that could indicate malware. Modern malware can evade traditional signature-based scanning, so watching how a running machine behaves is important. Events such as an attempt to call home to a command-and-control system may indicate an infection.

In addition to behavioral analysis, the solution also provides CVE vulnerability analysis to streamline recovery. The older a recovered snapshot is, the higher the likelihood that that machine is missing critical patches, which may be why malware was able to infect the system in the first place.

The recommended duration for the validation phase is at least 8 hours, during which time:

- Behavioral analysis continues to run, scanning for anomalous behaviors, such as running software that has a bad reputation, running processes that repeatedly make outbound connections, reaching out to known suspicious IP addresses, malicious interference with the Windows Registry, or other system files or processes on the VM.
- Network isolation levels can be modified, and impact observed.
- Patching can be completed and validated.
- Alerting of new risks will be provided in real time.

Once you have achieved a level of confidence that a recovered VM is in a good state, final steps for most recent data recovery, staging and recovery to source site can be easily and quickly managed.

Fine Tuning

This phase is optional, depending on the age of the data in the recovered snapshot. It is possible that the recovered snapshot contains data that is current enough to recover to production. On the other hand, if the most viable “clean” snapshot is 3 months old, it may be desirable to recover data from a newer snapshot to reduce the impact of the attack.

Using the Guest File Restore capability of VMware Cloud Disaster Recovery, it is possible to select data files from any snapshot in the machine’s history and pull the data into the cleaned and patched instance. While the machine is running in the IRE, behavioral analysis and malware scanning is in place, so if the newer data files contain known malware, that will be detected as they are restored.

Staging and Recovery

When a VM recovery is complete and has been badged as known-good, it is time to stage the machine for recovery to the source site. The following activities are performed:

- The VMware Carbon Black sensors are removed from the VM.
- The VM is powered down in the recovery SDDC.
- A final staging snapshot is taken, badged, and stored as an immutable snapshot in the SCFS.

It is likely that you will stage many VMs for recovery prior to recovering them to the source datacenter. This is because it may take time to remediate the source site, lock down end points, complete forensics, etc. Once those tasks are done, recovery is possible. This parallelism and batching facilitate quicker time to service recovery.

Once the source site has been cleaned and workload VMs have been staged for recovery and business resumption, it is very simple to select the in-scope and staged machines, confirm your intent to restore and overwrite the compromised source site machines with the clean, curated images, and power them up with automation. Based on how VCDR protects and recovers data. network data traffic and time to recover from the staged cloud snapshot will be fast and efficient as we only send required changed blocks to the source machine.

Conclusion

Recovering from a ransomware attack can be challenging, but with the right tools and processes in place, it can be done. A wellprepared incident response plan, deep restore point catalog, an isolated recovery environment, and administrator education are essential. Practicing recovery scenarios using the available tools and processes will ensure that teams are ready to respond. By prioritizing cybersecurity, being proactive, and building expertise, organizations can rebuild and regain control in the event of a successful malware attack.