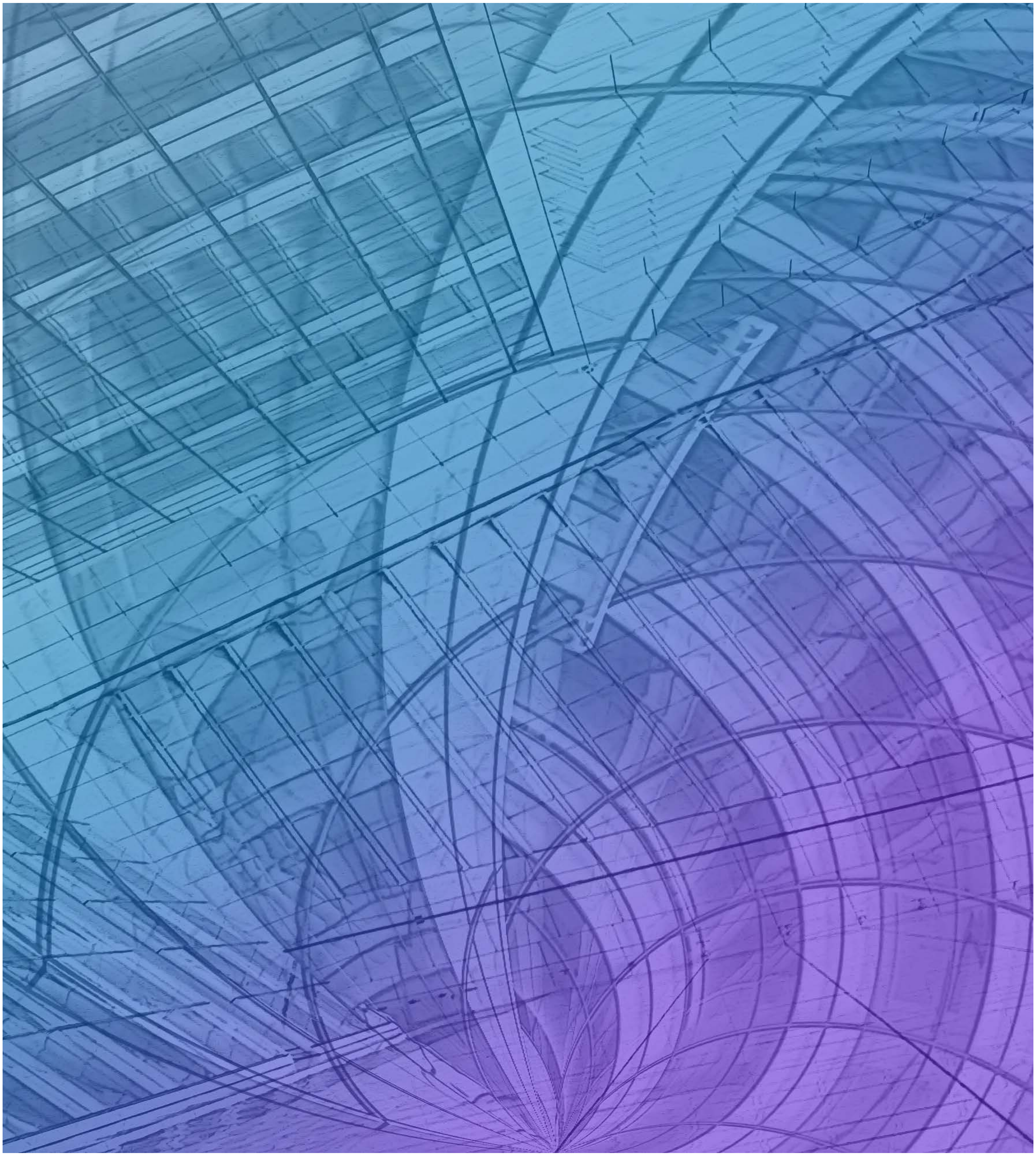
The Complete Ransomware Recovery Guide

Datrium®

WHITEPAPER



Contents

Introduction

This document covers what you need to know about ransomware and how to protect your VMware environment. It has detailed steps for proactive prevention, what to do when your systems are infected, and finally, how to recover from a ransomware attack. Using best practices for ransomware prevention, network intrusion, encryption, and anti-phishing tools, plus keeping all endpoints up to date with the latest security patches will put you in a good position to recover your data without paying a ransom.

Proactive Prevention: Ready for Recovery

Regardless of the precautions you take, someday you could be hit by ransomware.

Ransomware is a type of computer malware that denies users access to their systems or data. Once the malware is activated, a user can't access their critical data or use virtual machines (VMs). The attackers then demand a ransom with the promise (but not guarantee) of returning access to the affected systems or data. Most attackers demand that victims pay with online cryptocurrencies, such as Bitcoin.

To learn more about types of ransomware, attack patterns, prevention tools, and recovery mechanisms, read our Ransomware Recovery Stories and blog posts. You can also watch this webcast about how Datrium helped a midwestern city IT team recover quickly after a ransomware attack.

Ransomware is a serious threat because, as of today, no prevention tool has proved to be 100% effective against all known (and evolving) strains of ransomware. A model called Ransomware-as-a-Service (RaaS) has emerged that allows ransomware developers to recruit attackers who could launch millions of attacks aimed at organizations of all sizes across the globe. While we still recommend that our customers have updated endpoint protection tools in place, we want to highlight the fact that *recovery* is the only known protection against having to pay a ransom to the attackers.

What Can You Do?

To help prepare for a ransomware attack, you should have a plan in place *before* it occurs. If someone does hold your data for ransom, you can retrieve VMs and data stored in a *safe place* (on premises or in the cloud) and recover from the attack.

For VMware users, we recommend the following precautions for proactive ransomware prevention.

Develop and Follow Ransomware Protection Best Practices

In our experience, finding all the critical system passwords is the longest delay in recovering IT systems after a ransomware attack or other disaster. If you use a password manager/server for your critical systems, the ransomware may encrypt or lock this server. During recovery, the first step is getting access to the passwords for the remaining servers. You won't be able to recover quickly if you have to recover each server password in the domain. To accelerate the recovery process, we recommend that you identify and protect your critical passwords before the attack.

Identify Critical Passwords

In the event of a ransomware attack, you'll need access to critical passwords beyond your storage and vSphere domains and outside the compromised environment to restore your original systems during recovery.

You and a few trusted team members should have access to these passwords at all times:

- Storage admin
- Encryption
- vCenter
- ESXi
- Other critical VM credentials

Isolate Password Manager

If you use a password manager/server for your critical systems, we recommend that you don't include it in the same Active Directory (AD) domain as the rest of your servers because it could be susceptible to ransomware. If the password manager is within the attack surface, then additional hard copies of those passwords should be kept in a physically isolated, secure, yet accessible environment.

Plan and Configure Protection Groups

To help protect your data and fight potential ransomware attacks, we recommend you use Protection Groups (PGs) for your VMs and files. A PG contains one or more VMs and/or files from any host, and it defines snapshot schedules, snapshot retention policies, and replication and replica retention policies for the PG contents. Several backup and DR solutions have features to create and manage PGs. Your solution should allow you to create multiple PGs.

At a minimum, we recommend that you configure at least one PG with a membership of "*" to take at least a minimum daily snapshot with some duration of retention. No matter which backup and recovery tool you use, having this snapshot should be your first point-of-instant-recovery of your data from a ransomware event.

Protect Critical PGs With a 3-Tier Approach

To plan for recovery at the infrastructure, application, and data center level, we recommend a more robust strategy of PG creation and management.

A proposed *3-tier* approach for PGs could include:

- Tier 1 Recovery PG: vCenter Server, DNS Servers, Domain Controllers, NTP server
- Tier 2 Recovery PG: Other critical infrastructure services servers
- Tier 3+ Recovery PGs: Application or data-center level PGs built around applications or general VM workloads

Important:

- The ability to recover key infrastructure services separately, ahead of recovering applications and data, is a critical step to overall recovery.
- vCenter should be omitted from a PG that has 100% of the VMs, and it should be protected with its own dedicated PG for vCenter.

This approach is best when all of your systems, up to and including your vCenter and Domain Controllers, are affected by ransomware. Recovering those systems first will allow you to better prepare for restoring other systems.

The NTP time server is included in this group, as a recommended step, when recovering from malware. That's important because a ransomware *activation event* (point in time when your data or system becomes unavailable and a ransom message appears) is usually based on a date and time trigger. Restoring the NTP time server and then setting the time back a week (or more) may prevent an immediate recurrence of the ransomware *activation event*. That allows you to restore other affected VMs with a very low RPO.

As soon as the VMs boot, they should reset the system clock back to the pre-dated NTP server, which will give you time to recover your data or clean systems without having the ransomware cryptolock event take place immediately on the recovered machine.

Establish Your Backup Strategy

In the event of a ransomware attack, you need to go *back in time* to a last-known clean snapshot before the attack occurred, and restore your clean VMs and data quickly, with low RPO. To do that, your storage system should allow you to configure your snapshot frequently and support at least 2000 PG snapshots per group, and a total maximum of up to a million VM snapshots to ensure you can locally protect, and externally replicate, all of your essential VM data. Finally, your backups should be *immutable (can't be changed*), and each snapshot should provide a full restore/restart of each VM from any point in time.

Configure Snapshot Frequency of the PGs

A typical backup tool takes a snapshot once or twice a day. That's done to conserve storage space and data egress charges (for cloud backups). For effective ransomware recovery, we recommend you take VM- or PG-level snapshots as often as necessary to meet your organization's RPO goals. Snapshots should be instantaneous and provide a crash-consistent point in time for all VMs in a PG. There should also be no VM Guest impact when taking a snapshot.

We recommend using backup systems that let you create a snapshot schedule at a set frequency (at least 10 minutes), so the snapshots can capture critical data over time and be used to restore in the event of data loss or a ransomware attack.

Consider the following points as you decide on the snapshot schedule frequency for a PG.

How Frequently Do the VMs In Your PG Change?

If you have VMs for an application that changes frequently, and each of those changes is potentially important, you may want to create a more frequent snapshot schedule, so you have more options to choose from when you pick a saved snapshot to restore.

For example, with non-I/O intensive VMs, such as web or application servers where the server state does not change frequently, it may be optimal to set a longer snapshot frequency. But for applications that are I/O intensive and have rapid data changes, such as a mail server or a database server, you'll want to create a more frequent snapshot schedule.

How Much Storage Is Available?

Every application has its own data storage needs. For applications that store a lot of data, and therefore require a lot of storage to keep running, you may want to create a less frequent snapshot schedule to avoid running out of backup space that's required for replication.

Keep in mind that each snapshot should be able to serve as a standalone backup, so there's no dependency between snapshots or upon the snapped object. That allows you to specify different retention periods for snapshots and protected sites (if replicated). You can retain snapshots for as long as necessary, even if the original object upon which the snapshot was based no longer exists.

Protect Locally, Replicate Externally With Replica Sites

Typical backup tools allow you to add a replica (or replication) site that will receive and store snapshot replicas to another protected on-premises environment, off-premises secondary site, or the cloud. We recommend replicating snapshots externally to a secure, low-cost cloud option, such as AWS S3. After you add the replica site, you can reference the site in PG schedules or manual replication operations when you need it.

Ensure Each Snapshot Is Immutable and VMs Are Fully Recoverable

Because ransomware can encrypt data on network drives, the snapshots must be stored in a safe location, so each snapshot is immutable. We recommend using a backup solution that allows you to store data off premises in a secondary site or the cloud. Your backups should be inaccessible and undecryptable by any malware.

Establish Your Retention Strategy

A ransomware infection can live in your system for weeks or even months before the actual *activation event*. To successfully recover, you need to design a retention strategy that gives you many recovery points while keeping backups for the longest time at a reasonable cost. We recommend you consider a solution that gives you the flexibility to configure retention time and backup frequency with an easy-to-use UI.

Local Retention Time Considerations

When you take a snapshot or create a snapshot schedule, we recommend setting an expiration for the snapshot, so after a given amount of time, the snapshot is deleted. You should also be able to configure the snapshot to *never* expire. For successful ransomware recovery, every snapshot should be a synthetic full backup of each VM, and the data being protected must be immutable.

Ideally, the software functionality to manage and retain snapshots should be included at no charge in your backup and recovery tool. Please note that leveraging snapshots will consume additional storage capacity. Typically, when data in a VM is overwritten (without snapshots in place), it will eventually be removed from the system. If snapshots are enabled for a VM, overwritten data is saved because it's protected by snapshots. Storing these backups consumes capacity in your backup system and is variable depending on snapshot frequency, retention policy, and data change rates over time.

Retention Periods – Monthly, Weekly, Daily, or Hourly?

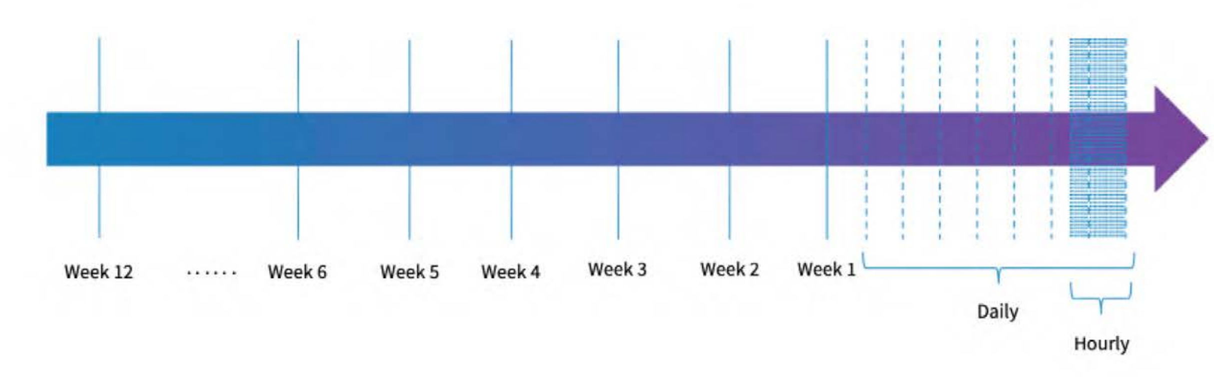
An organization should retain immutable backup data for at least six months, according to a study by RSA and Secureworks on best practices for ransomware protection. That's because of the insidious nature of many ransomware infections. They may actually take place over several months before being discovered, create an adverse scenario, or physically remove access to files.

While a best practice includes long-term retention for critical systems, short-term retention for very frequent (daily or hourly) snapshots of systems can add to that protection without exhausting the storage space.

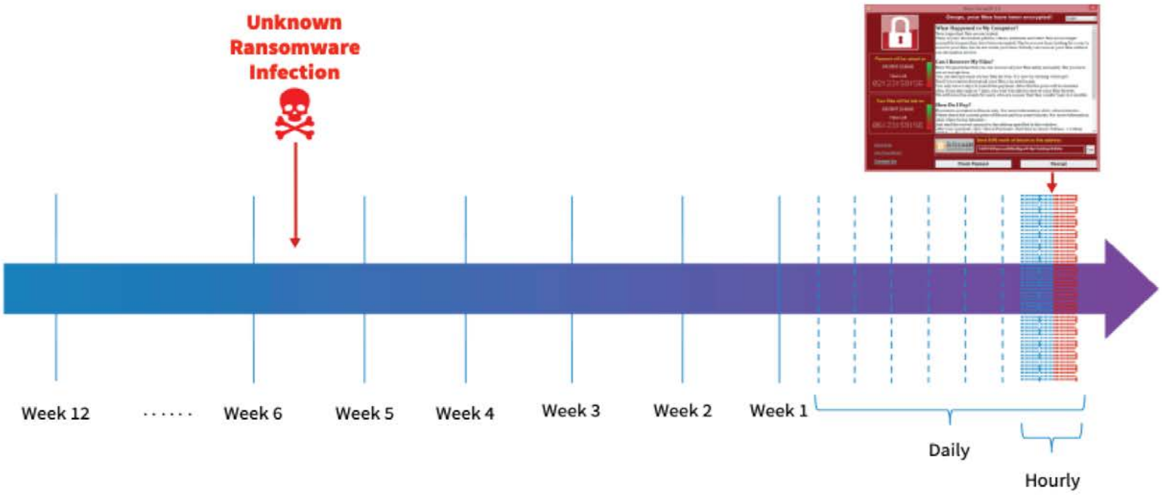
- **Weekly snapshots and monthly retention**: Allows potential recovery of VM operating system, applications, and data from many months ago before an infection
- **Daily and hourly snapshots with daily or hourly retention**: Allows for potential recovery of data with a very low RPO to minimize data loss when there's a cryptolock event and access to filesystem data is removed

Example Retention Schedule:

Each line indicates a retained snapshot with a defined retention period.



With this type of protection schema, it could provide the most robust recovery prospects from a ransomware infection:



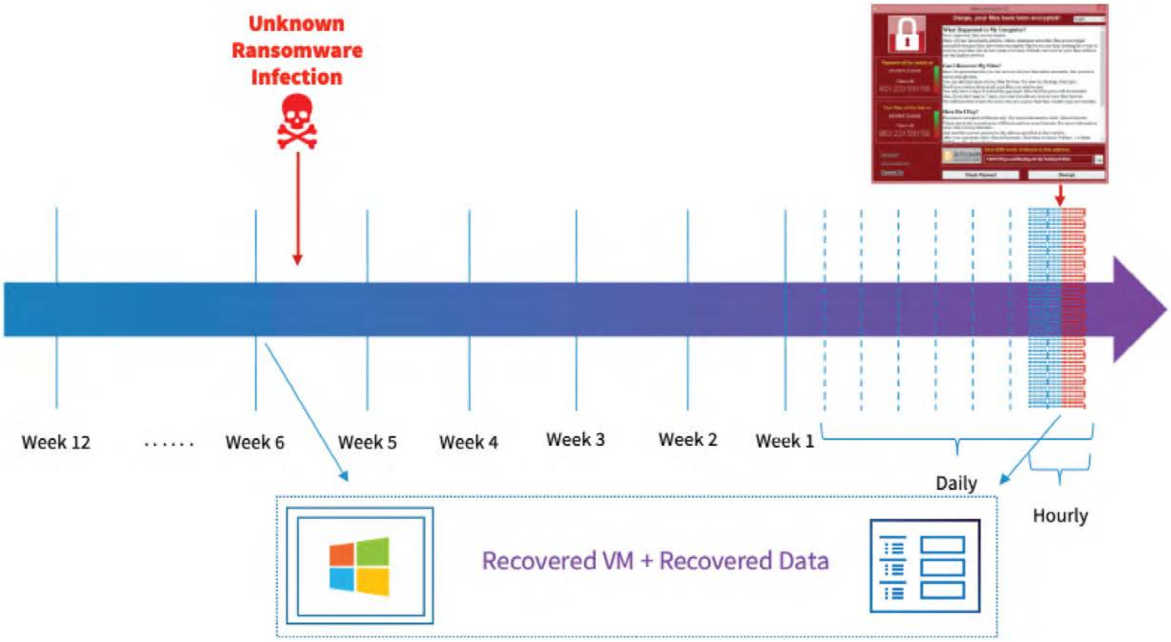
In the example above, the actual ransomware infection may have occurred 5-6 weeks prior, but it went unnoticed. During that time, filesystems may have been encrypted but still available. Also, during this period, if the infection is not noticed, the malware is most likely encrypting local filesystems but also searching the network to find and encrypt other vulnerable targets, including NFS- and CIFS-based backup servers and repositories.

Ultimately, when the ransomware payload activates (as pictured above – roughly 5 hours earlier), all data access across platforms will likely be removed. Subsequent snapshots taken after the payload activation (in red above) will be snapshots of the newly encrypted system. The immutable snapshots from immediately before the event still have accessible data and are immediately restorable, so you don't have to pay the ransom.

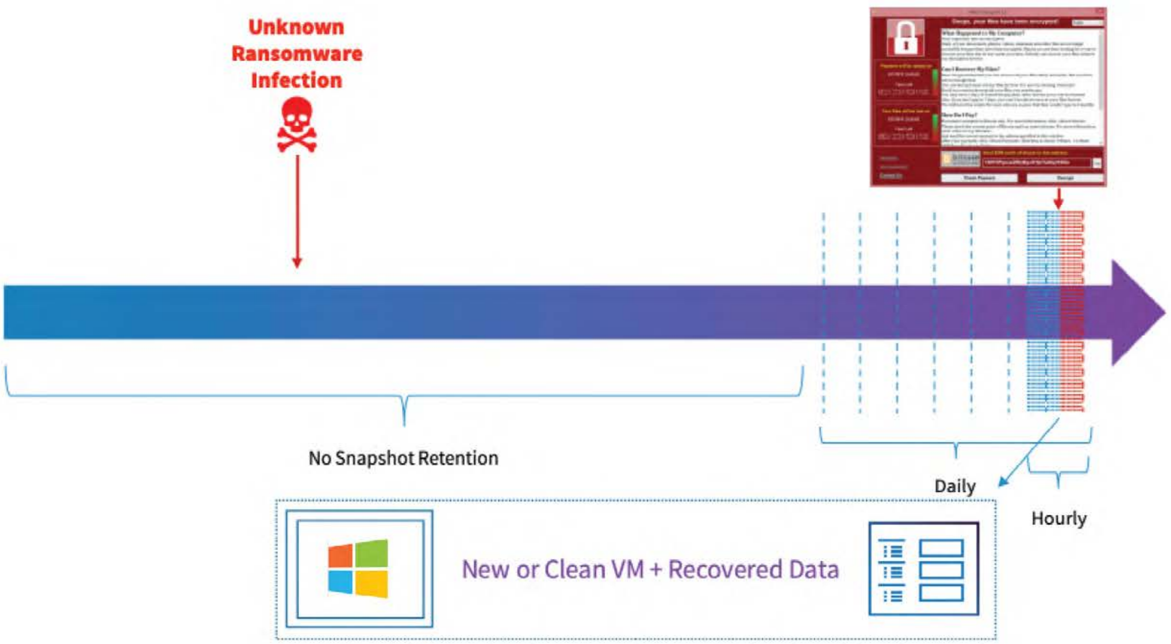
As illustrated in this example, you have multiple options to restore.

In summary:

Restore a clean OS image/application from Week 6 snapshot, restore data from 6 hours ago, recover the data to the clean OS image



- **Important**: If retention was only set for hours or days and long-term retention of weekly snapshots wasn't enabled, restoring a snapshot from before the ransomware activation is a guaranteed low RPO option to recover data, *but* the data itself is still sitting on an infected OS. Once recovered, the data should be moved to a clean target for safekeeping, and the infected VM should be rebuilt or otherwise cleaned before being returned to service.

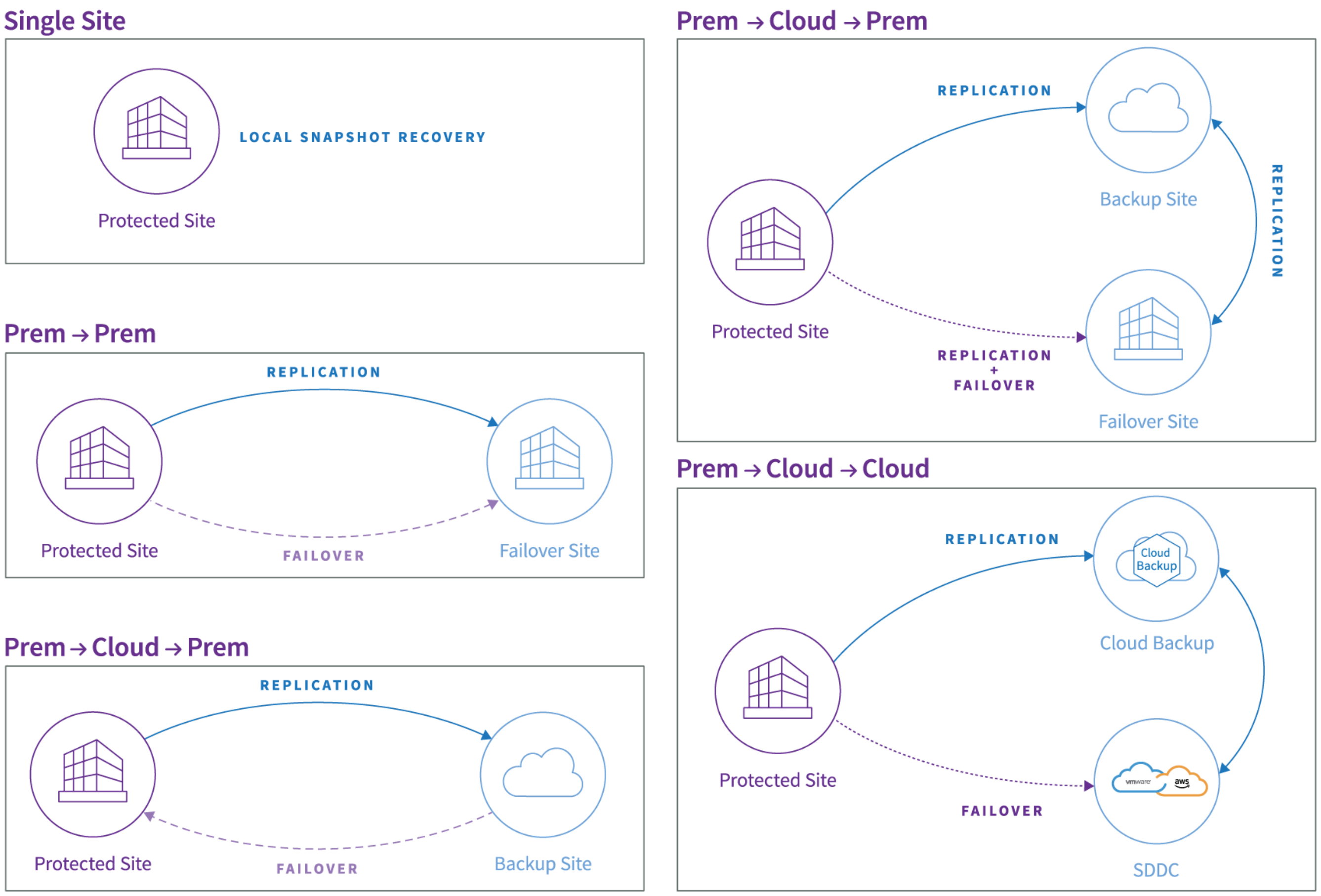

Unknown Ransomware Infection
No Snapshot Retention
Daily
Hourly
New or Clean VM + Recovered Data

Given the above example, here are some factors that affect the answer to how long you should retain snapshots locally or replicate to a secure site:

- Space considerations: what are the retention length, data quantity, and data change rate? Retaining a large number of snapshots with a high change rate for an extended duration will consume additional capacity and may cause space constraints or require capacity upgrades.
- What are the compliance and recovery objectives of your organization?
- Is it feasible for your organization to recover older (clean) OS images and move recovered data to those old images?
- Is it more feasible to clean or rebuild infected VMs after you have recovered data?

Replication and Data Protection Topologies

Please confirm that your backup tool provides many options for onsite, offsite, and cloud data protection and recovery to meet your organization's needs. Below are some of the suggested topologies:



Single Site

Prem → Prem

Prem → Cloud → Prem

Prem → Cloud → Prem

Prem → Cloud → Cloud

Regardless of the location of your site and replication topology, all your protected data should be:

- Immutable
- Universally deduplicated and available across all sites
- Part of a universal catalog in which every protected system (source or target) knows about your data retention strategy and location of protected data

To recover from ransomware, any of the topologies identified will work as long as your DR solution allows you to recover local snapshots in a data center, snapshots from a remote site or the cloud to a primary data center, snapshots at a secondary location, or to a clean vCenter in the public cloud by leveraging cloud backup and orchestration for automated cloud recovery.

In-Place Recovery

In a single site topology, one system serves as both the primary and recovery system. Your solution should provide persistent and highly-available storage for active data sets and also store all immutable snapshot data in a local pool. It should also store snapshot catalog data in an immutable database to ensure access to snapshots.

The administrator should be able to recover any snapshot for any VM or PG from any available snapshot for immediate restart from that point in time using the vSphere Plugin GUI or your solution's GUI.

Single-site topology is optimal for:

- Recovering in-place VMs to a known good point in time
- Fastest, least disruptive recovery
- Low RTO – VM restart on recovery sites (without having to copy backups) by using ongoing replication

Prem to Prem

In this topology, you have two storage systems in different locations, and one (the protected site) sends snapshot replicas to both the failover site and a backup site because replication schedules and retention policies don't need to be the same.

This topology is useful for extra protection, longer archiving, or as a method of recovering from ransomware attacks that require going *back in time*, which a failover site alone might not be able to accommodate if it has a shorter local retention period.

This topology is optimal for:

- Incidents that render infrastructure outside of the VMware environment inaccessible, such as network devices, where offsite recovery is most advantageous
- Testing features within DR orchestration that can be used for proving remediation efforts before attempting those actions in the live environment

Prem to Cloud

This topology combines the economic benefits of eliminating a secondary DR site with the low RTO recovery to the public cloud.

For this topology to work, your DR solution should have a cloud backup site. In this case, following a disaster event, a failover site is deployed in the public cloud – for example, VMware Cloud on AWS. A DR plan will perform a failover to this newly created cloud failover site.

This topology is optimal for:

- Incidents that render infrastructure outside of the VMware environment inaccessible, such as network devices
- Testing features within a DR solution before deploying it in the live environment

Establish a DR Plan for Automated Recovery

We recommend you use a DR solution that supports an orchestration capability, which allows you to create a DR Plan for automated recovery of individual VMs or entire sites from any available snapshot with near-zero RTO – regardless of whether the selected recovery point is recent or older. The ability to orchestrate recovery from older snapshots is a particular advantage in ransomware scenarios where it's necessary to go *back in time* (sometimes months) to identify uninfected data.

Here's how DR orchestration can help you during an attack:

- Test resolution measures in an isolated sandbox before you deploy them on the live environment
- Recover outside the compromised environment when a malware incident has compromised the environment beyond the DR solution and vSphere domains
- Quickly and easily create an environment for security tools where personnel from federal, state, or local government agencies, such as the FBI, can perform forensics
- Use the option for site-to-site recovery to a separate clean or newly built infrastructure that's not affected (or less affected) by the ransomware event
- Recover using the option for site-to-cloud recovery using on-demand VMware Cloud

What to Do When Your Systems Are Infected

Step 1: Isolate Infected Computer(s) Immediately

You should immediately isolate and disconnect the infected systems:

- Disconnect VM vNICs from the network.
- **If you are using Datrium products, don't shut down your Datrium Data Nodes**, as this will slow down your recovery efforts.
- Even if your VMware environment and vCenter are not online or available, check if you can use your HCI or DHCI GUI to:
    - Disconnect hosts
    - Extend retention on most recent or other critical snapshots
- Outside the core server infrastructure, here are other suggestions:
    - Start disconnecting connections or implementing strict whitelists for internet, WAN connections, or end users – this will potentially spare systems not already affected and also isolate potential *spawners of the attack*, which may re-infect clean systems as they are restored.
    - Generally, it may not be a good idea to shut down your core switches because that could remove all ILO / DRAAC connectivity and prohibit your recovery.
    - Shutting down network systems might remove non-persistent network logs that may help with forensic analysis of attack source and vector.

Step 2: Immediately Secure Backup Data or Systems by Taking Them Offline

Isolate your backup software or data retention systems, and if they are not impacted, ensure that they are locked down to prevent encryption or loss of access.

If you're using backup on Windows or Linux media server, NFS, or sysmount, it's very likely that these platforms have already been locked down. We recommend that you take them offline anyway.

Because ransomware infection may lie undetected for weeks or months, we recommend that you stop your backup tool from expiring snapshots. It ensures that older snapshots will be available if needed.

Note: Stopping snapshot expiration will cause increased space consumption.

When hosts are isolated (to prevent further spread of malware or re-infection), and snapshot expiration has been suspended, it's time to execute your recovery plan.

Subsequent sections describe how to recover your data and provide forensics to insurance adjusters, regulatory agencies, or law enforcement agencies.

Note: Simply recovering your VMs, applications, and data is only part of an organization-wide recovery effort.

Before executing an actual data recovery, other significant tasks may be required. Please verify the following:

- Has the source of infection been isolated and removed? For example, is it still being installed via AD policies?
- Is the network available and secure?
- Are IT administrator endpoints online, clean, and available?
- Are other IT systems isolated or in a pre-recovery state?

This list is not exhaustive, and every scenario will be different. Once you have executed a plan to prepare for data recovery, you can proceed.

Executing Data Recovery

Step 3: Forensic Work

Whether or not your ransomware event becomes public, your corporate audit and information security teams will likely spearhead coordination and communications with local, state, and federal law enforcement.

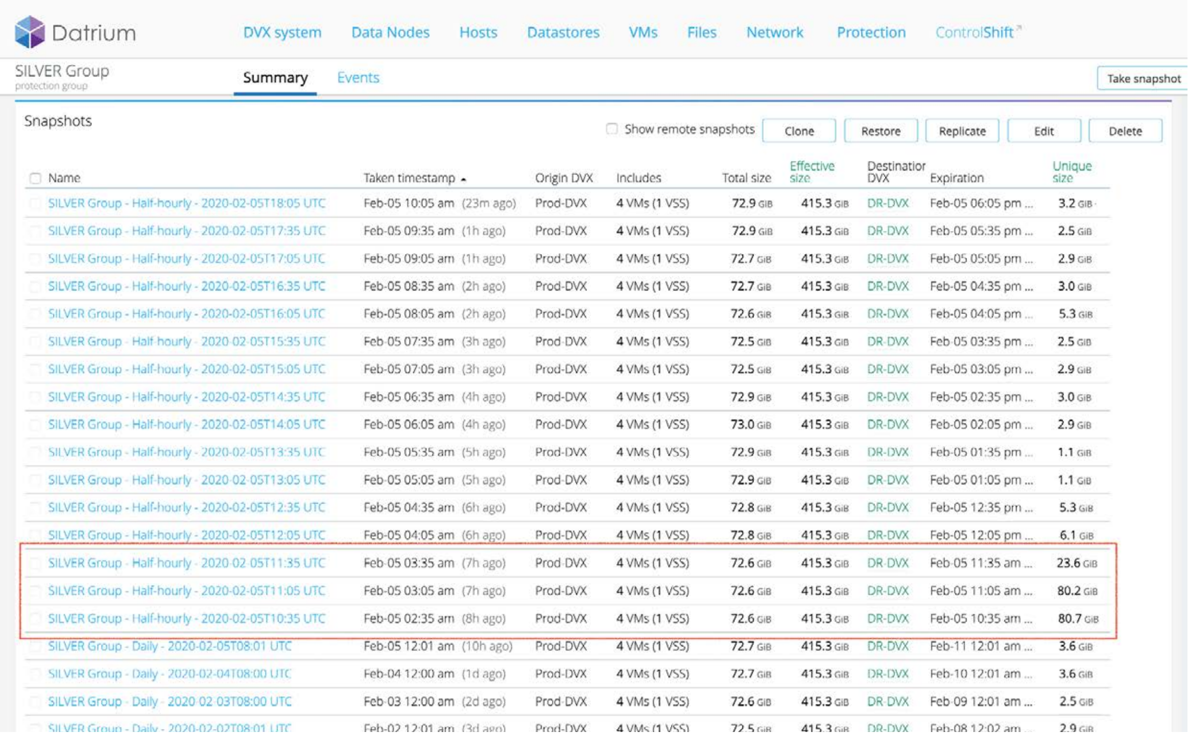
Insurance auditors and other involved parties, including law enforcement, will likely work with you to determine the source of the ransomware attack. It will be critical for recovery and prevention of future attacks to understand how the breach of your IT systems was achieved.

For these purposes, identifying and preserving key forensic data may be critical operationally, legally, and financially.

Your backup solution can help pinpoint the initial timeframe of the system infections. You may notice in the capacity reports that there was a significant growth in snapshot space requirements as VMs were being encrypted before being locked out.

Steps to identify and recover from the attack point:

- Identify snapshots that have been compromised.
    - One thing to check is unique data written. If encryption was sudden, unique data in snapshots would jump significantly.
- Restore snapshots in quarantine (no networking), validate if compromised.
- Identify the source of ransomware dissemination, if possible.
- Rectify the environment's vulnerabilities.
    - If possible, change all online account passwords and network passwords after removing the system from the network.
- Extend retention time on uncompromised PGs or create clones of those snapshots with no expiration time and date.
    - It's critical to either extend the retention time or set them not to expire to make sure the snapshots are retained for the duration of recovery and forensics work. If snapshot expiration is not changed, the system will clean them up per the expiration schedule, and they will not be recoverable.



□ Name	Taken timestamp ▴	Origin DVX	Includes	Total size	Effective size	Destinatior DVX	Expiration	Unique size
SILVER Group - Half-hourly - 2020-02-05T18:05 UTC	Feb-05 10:05 am (23m ago)	Prod-DVX	4 VMs (1 VSS)	72.9 GiB	415.3 GiB	DR-DVX	Feb-05 06:05 pm ...	3.2 GiB
SILVER Group - Half-hourly - 2020-02-05T17:35 UTC	Feb-05 09:35 am (1h ago)	Prod-DVX	4 VMs (1 VSS)	72.9 GiB	415.3 GiB	DR-DVX	Feb-05 05:35 pm ...	2.5 GiB
SILVER Group - Half-hourly - 2020-02-05T17:05 UTC	Feb-05 09:05 am (1h ago)	Prod-DVX	4 VMs (1 VSS)	72.7 GiB	415.3 GiB	DR-DVX	Feb-05 05:05 pm ...	2.9 GiB
SILVER Group - Half-hourly - 2020-02-05T16:35 UTC	Feb-05 08:35 am (2h ago)	Prod-DVX	4 VMs (1 VSS)	72.7 GiB	415.3 GiB	DR-DVX	Feb-05 04:35 pm ...	3.0 GiB
SILVER Group - Half-hourly - 2020-02-05T16:05 UTC	Feb-05 08:05 am (2h ago)	Prod-DVX	4 VMs (1 VSS)	72.6 GiB	415.3 GiB	DR-DVX	Feb-05 04:05 pm ...	5.3 GiB
SILVER Group - Half-hourly - 2020-02-05T15:35 UTC	Feb-05 07:35 am (3h ago)	Prod-DVX	4 VMs (1 VSS)	72.5 GiB	415.3 GiB	DR-DVX	Feb-05 03:35 pm ...	2.5 GiB
SILVER Group - Half-hourly - 2020-02-05T15:05 UTC	Feb-05 07:05 am (3h ago)	Prod-DVX	4 VMs (1 VSS)	72.5 GiB	415.3 GiB	DR-DVX	Feb-05 03:05 pm ...	2.9 GiB
SILVER Group - Half-hourly - 2020-02-05T14:35 UTC	Feb-05 06:35 am (4h ago)	Prod-DVX	4 VMs (1 VSS)	72.9 GiB	415.3 GiB	DR-DVX	Feb-05 02:35 pm ...	3.0 GiB
SILVER Group - Half-hourly - 2020-02-05T14:05 UTC	Feb-05 06:05 am (4h ago)	Prod-DVX	4 VMs (1 VSS)	73.0 GiB	415.3 GiB	DR-DVX	Feb-05 02:05 pm ...	2.9 GiB
SILVER Group - Half-hourly - 2020-02-05T13:35 UTC	Feb-05 05:35 am (5h ago)	Prod-DVX	4 VMs (1 VSS)	72.9 GiB	415.3 GiB	DR-DVX	Feb-05 01:35 pm ...	1.1 GiB
SILVER Group - Half-hourly - 2020-02-05T13:05 UTC	Feb-05 05:05 am (5h ago)	Prod-DVX	4 VMs (1 VSS)	72.9 GiB	415.3 GiB	DR-DVX	Feb-05 01:05 pm ...	1.1 GiB
SILVER Group - Half-hourly - 2020-02-05T12:35 UTC	Feb-05 04:35 am (6h ago)	Prod-DVX	4 VMs (1 VSS)	72.8 GiB	415.3 GiB	DR-DVX	Feb-05 12:35 pm ...	5.3 GiB
SILVER Group - Half-hourly - 2020-02-05T12:05 UTC	Feb-05 04:05 am (6h ago)	Prod-DVX	4 VMs (1 VSS)	72.8 GiB	415.3 GiB	DR-DVX	Feb-05 12:05 pm ...	6.1 GiB
SILVER Group - Half-hourly - 2020-02-05T11:35 UTC	Feb-05 03:35 am (7h ago)	Prod-DVX	4 VMs (1 VSS)	72.6 GiB	415.3 GiB	DR-DVX	Feb-05 11:35 am ...	23.6 GiB
SILVER Group - Half-hourly - 2020-02-05T11:05 UTC	Feb-05 03:05 am (7h ago)	Prod-DVX	4 VMs (1 VSS)	72.6 GiB	415.3 GiB	DR-DVX	Feb-05 11:05 am ...	80.2 GiB
SILVER Group - Half-hourly - 2020-02-05T10:35 UTC	Feb-05 02:35 am (8h ago)	Prod-DVX	4 VMs (1 VSS)	72.6 GiB	415.3 GiB	DR-DVX	Feb-05 10:35 am ...	80.7 GiB
SILVER Group - Daily - 2020-02-05T08:01 UTC	Feb-05 12:01 am (10h ago)	Prod-DVX	4 VMs (1 VSS)	72.7 GiB	415.3 GiB	DR-DVX	Feb-11 12:01 am ...	3.6 GiB
SILVER Group - Daily - 2020-02-04T08:00 UTC	Feb-04 12:00 am (1d ago)	Prod-DVX	4 VMs (1 VSS)	72.7 GiB	415.3 GiB	DR-DVX	Feb-10 12:01 am ...	3.6 GiB
SILVER Group - Daily - 2020-02-03T08:00 UTC	Feb-03 12:00 am (2d ago)	Prod-DVX	4 VMs (1 VSS)	72.6 GiB	415.3 GiB	DR-DVX	Feb-09 12:01 am ...	2.5 GiB
SILVER Group - Daily - 2020-02-02T08:01 UTC	Feb-02 12:01 am (3d ago)	Prod-DVX	4 VMs (1 VSS)	72.5 GiB	415.3 GiB	DR-DVX	Feb-08 12:02 am ...	2.9 GiB

An Example of a Ransomware-Caused Anomaly in Unique Snapshot Size

Step 4: Begin Recovery

If you're the victim of a ransomware attack, you can leverage snapshots on a destination site (either a different site or the original restored site) to resume normal operations.

To recover VMs and files from snapshots:

- Determine the timestamp of the ransomware encryption event.
- Restore the latest pre-encryption event snapshots for most recent data.
- Find the timestamp of the ransomware infection event.
- Mark the latest pre-infection event VM, application, or operating system as the *golden image*.
- Clone from these golden images and restore VMs to get a clean, ransomware-free environment in your recovery site.
- Recover more recent data to the clean VMs you just restarted in your recovery site.

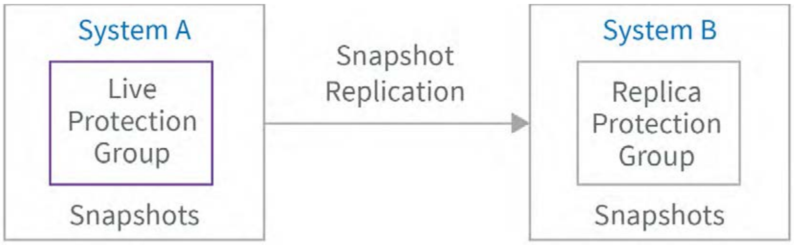
Points to consider before restoring snapshots:

- Once a snapshot has been verified as uncompromised, it should be cloned, or the VM should be restored in a clean environment. See Cloning below for more information.
- On restore, we recommend taking a new snapshot of VM's current state. This snapshot's drives can be provided as forensic evidence.
  - It may be desirable to set a longer retention time on the forensic snapshot.
- After uncompromised PGs have extended retention times, re-enable snapshot expirations.

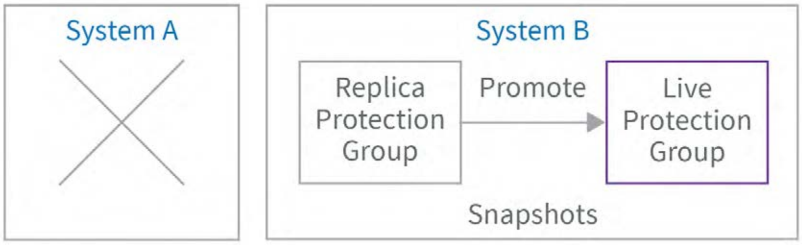
Disaster Recovery Example

This example illustrates a DR configuration and recovery for a prem-to-prem topology, with one site as the protected site, and the second as the replica site.

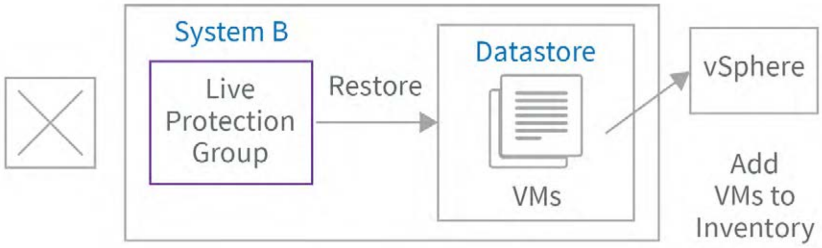
1. During normal operations, system A is the source system in a replication pair. It produces and replicates snapshots to the destination system B.



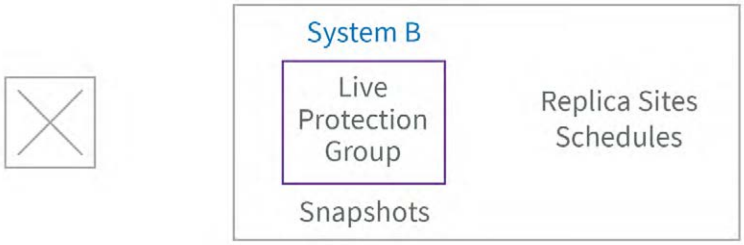
2. If system A goes down, start the recovery on system B



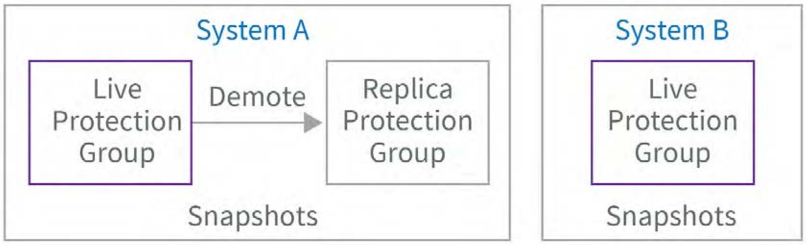
3. On system B, use a snapshot to restore the PG contents.



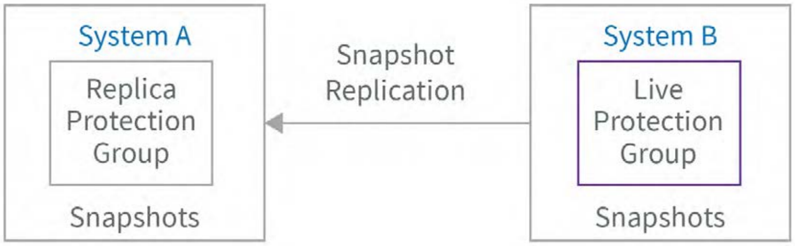
4. To complete the recovery:
   - Make sure that the original source system is marked as a replica site.
   - Add a replica site reference to the snapshot schedule(s).



5. When the original source (system A) is operational, demote the original source PG, so only system B has the live PGs in your environment.



6. Enable the schedule(s) for the live PG. When snapshot operations are performed on system B, it should send snapshot replicas to system A.



Step 5: Recover PG Content

When you recover PGs, you'll perform these general tasks:

1. Promote
2. Select a PG to promote.
3. Promote to make it live.

Restore

1. Select a snapshot you'd like to recover from and restore it.
2. Add any VMs to the vSphere inventory manually, if it's not done automatically.

Demote

1. Select the source PG on system A and demote it to ensure there's only one live PG at a time.

Step 6: Clone From Snapshots

When necessary, you should clone snapshots to provide them to the government authorities or others for analysis. Your tool should support a clone operation to create one or more VMs and/or files to be used for forensics.

After you've restored snapshots following an attack, you should create clones of:

- A VM from a VM instance
- A VM from a VM snapshot
- The contents of a PG from a PG snapshot

It's important to note that a typical cloning process will create a point-in-time copy of that VM from the snapshot selected. These VM clones are usually unique and have a new vCenter UUID. It's **not recommended** that you register these in vCenter or start them, but you should extend their retention until they can be exported and provided to appropriate authorities or insurance adjusters.

To be eligible to file claims, many insurance policies for business impact of malware and IT data loss require that clients provide log and evidentiary data of infection.

Clone VM from a VM instance

Please follow the instructions in your tool's user guide to clone an instance of a VM.

Note: You may need to add the VM clone to the vSphere inventory manually.

Clone a VM Snapshot

Please follow the instructions in your tool's user guide to clone a VM from a VM snapshot.

Note: You may need to add the VM clone to the vSphere inventory manually.

Clone a PG Snapshot

Please follow the instructions in your tool's user guide to clone a PG snapshot:

Note: You may need to add any VM clones in the PG to the vSphere inventory manually.

An Introduction to Datrium's Ransomware Recovery Products

Datrium has helped many organizations reduce the risk of ransomware attacks and avoid paying the attackers. Our ransomware protection solutions include Datrium Disaster Recovery as a Service (DRaaS) with VMware Cloud on AWS and Datrium DVX.

DRaaS with VMware Cloud on AWS

DRaaS with VMware Cloud on AWS provides on-demand, failproof DR for all VMware workloads. It makes DR easy and reliable with its cloud-native design, built-in backup, instant RTO, and on-demand model. DRaaS allows you to manage a ransomware attack by instantly implementing a phased recovery, with mission-critical applications reinstated rapidly in a known clean environment while you clean up your everyday infrastructure.

For rapid ransomware recovery, DRaaS enables you to:

- Identify ransomware attack and activation events
- Create a 3-tier approach for your PGs
- Establish backup policies for low RPO and create tamperproof backups every few minutes, every hour, every day – whatever frequency makes sense for your business
- Establish low RPO retention policies with an intuitive UI
- Create any replication and data protection topology, including single site, prem to prem, prem to cloud to prem, and prem to cloud to cloud
- Create a DR plan or runbooks for automated recovery
- Execute a phased recovery in the event of a disaster

The stored backups are instantly powered on via a live cloud-native NFS datastore mounted by ESXi hosts in that SDDC, resulting in instant RTO. Unlike legacy backup-only solutions, there's no time wasted waiting for backup data to be copied into an SDDC before the VMs can be restarted.

Plus, there's no learning curve for IT teams. They use the same vCenter tools to manage their on-premises storage and cloud resources. Once the disaster is over, failback is easy too – deduplicated, changed data is compressed and encrypted, which minimizes egress charges, and then it's automatically sent back to the data center.

To learn more about Datrium DRaaS with VMware Cloud on AWS, please visit www.datrium.com/products/draas.

DVX

Datrium DVX is the leading disaggregated HCI (DHCI) solution in the market today. It's the industry's fastest and most resilient DHCI system, with built-in Blanket Encryption, backup, market-leading cost efficiency, and seamless integration with Datrium DRaaS.

For ransomware protection, DVX supports multiple replication and data protection topologies, including Single-Site and Prem-Prem topologies. When used with Datrium DRaaS, DVX also supports Prem-Cloud-Prem and Prem-Cloud-Cloud topologies.

Under the hood, DVX separates application data from recovery copies, increasing protection in ransomware situations. When data is stored in DVX, the virtualization layer stores that data in an NFS share with the industry's highest aggregate performance for consolidated VM storage – we call that namespace a datastore.

Datastores can be explicitly exported to different hosts by IP range, and those hosts can't access files in a separate datastore. Inline and lower in the stack, data is stored in a shared data pool that is globally deduped, compressed, and encrypted by the hosts, and it's saved with no overwrites of good data ever. Because DVX snapshots can't be reached through this process and aren't accessible to applications, they provide superior protection from ransomware.

To learn more about DVX, please visit www.datrium.com/products/dvx.

Additional Resources

Here are Datrium and third-party resources that will help you learn more about ransomware protection and recovery.

- Webcast – Ransomware: What It Is and How to Defend Against It
- Webcast – Ransomware: Top 3 Secrets Revealed
- Webcast – How to Recover Faster from a Ransomware Attack with On-Demand DR
- Webcast – 3 Must-Have Items for Your Ransomware Attack Readiness Checklist
- Blog – 6 Steps Ransomware Attackers Use
- Blog – 3 Numbers That Convinced Me That Ransomware Is a Threat
- Ransomware Prevention and Response for CISOs – U.S. Federal Bureau of Investigation (FBI)
- Cybersecurity and Infrastructure Security Agency (CISA) – The Department of Homeland Security

Summary

Thank you for reading this guide. Our mission is to empower people to fight against the threat of ransomware. We sincerely hope that you will never have to deal with the impact of a network breach due to ransomware or malware, but if you do, we're confident that the proven strategies discussed in this guide will enable you to recover your workloads after an attack.

Datrium has helped dozens of customers recover from ransomware – almost instantly and always without having to pay the attackers a dime. We want to make sure that our team and products help you too.

While Datrium's technology will help you recover your data in the event of an attack, there are many other areas of IT safeguarding and requirements that are necessary to prepare for and recover from an attack. We have your back when it comes to recovering your data from immutable storage with world-class RTO and RPO options. We can't predict which method of recovery will work best for your organization. Many of our customers have been able to locate the infection payload start time, clean, and restart quickly. Others have chosen to restart with reset clock times to safely pull the latest data before the infection locked it down.

Please take time to familiarize yourself with this runbook and follow the recommended guidelines, so you're always in a *prepared state* for recovery. Then, when you need it, you'll have it on the shelf to use for a fast and organized recovery.

To learn more about ransomware and how we can help, please visit www.datrium.com/solutions/ransomware-protection.

To learn more about Datrium, please visit www.datrium.com.

If you have any questions, feedback, or recommendations on this runbook, please email us at ransomware-protection@datrium.com

Thank you!

Brett Foy
Global VP, Sales Engineering