VEEAM

7 Best Practices for Ransomware Recovery

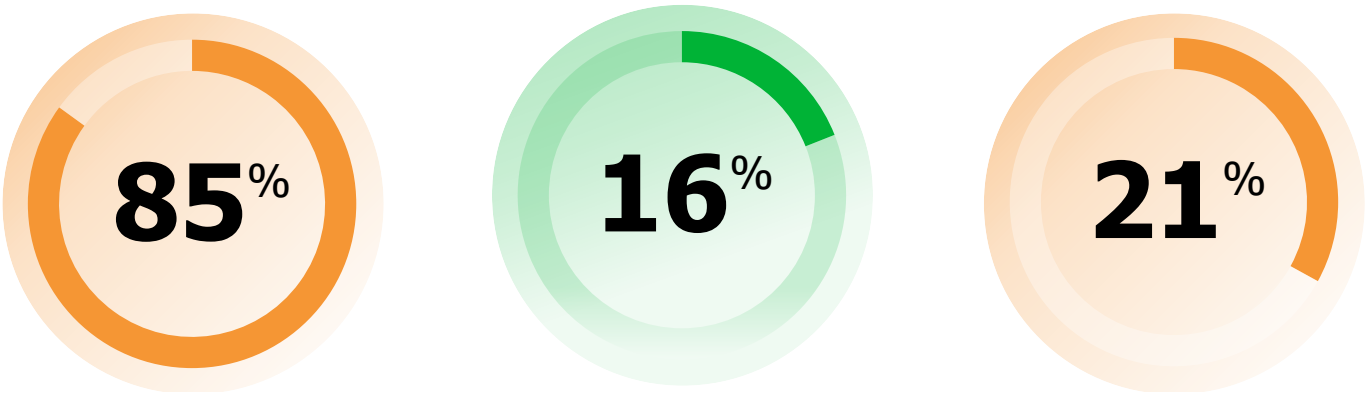
How to make recovery your top priority

Contents

Introduction: Ransomware is the worst kind of disaster

In recent years, ransomware attacks have become increasingly frequent and sophisticated, posing an increasing threat to organizations of all sizes and industries. The impact of a ransomware attack can be devastating, causing operational disruption, financial loss, reputational damage and potential legal and regulatory repercussions. Therefore, it's critical for executives to have a clear and comprehensive plan for ransomware recovery that can minimize the impact of an attack and restore business operations as quickly as possible.

According to Veeam's 2023 Data Protection and Ransomware Trends report:



of companies have experienced at least 1 ransomware attack in the past year

of companies were able to recover without paying the ransom

of companies paid the ransom but didn't recover their data

*Source: Data Protection Trends Report 2023, Ransomware Trends Report 2023

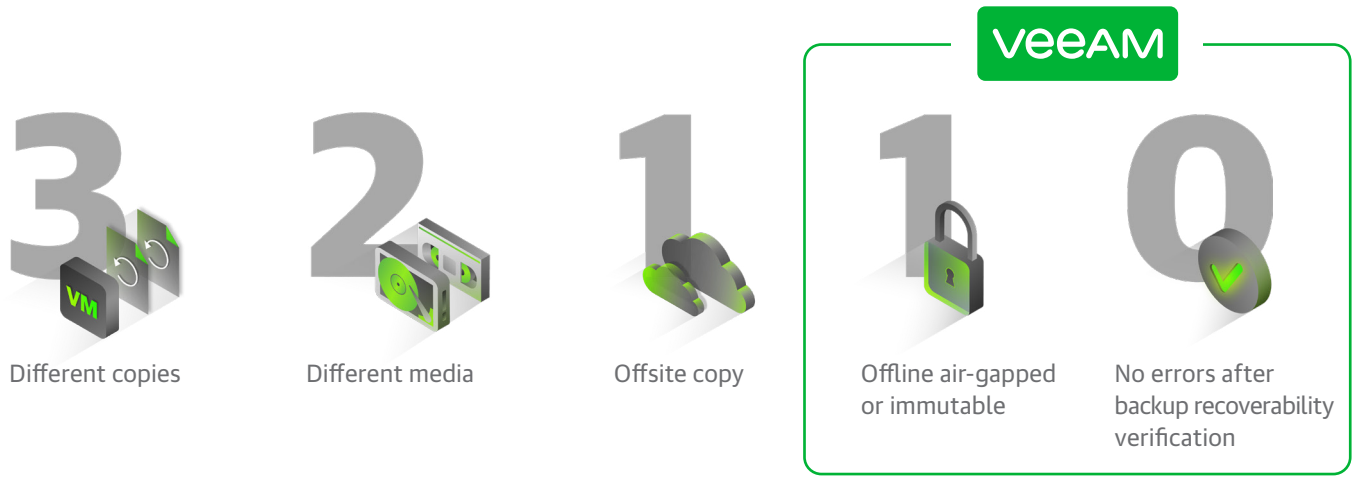
It's not possible to prevent every cyberattack, so organizations need to make recovery a priority. Backups are widely established as one of the most effective defenses against ransomware attacks. Having a recent, validated and secure backup increases the possibility of successful recovery while reducing downtime and minimizing the possibility of data loss.

Historically, disaster recovery (DR) planning has been viewed as part of an overall infrastructure plan. This then created assumptions around the integrity and availability of data during a crisis. Risk calculations have been based on antiquated statistics for data recovery, where only **3%** to **5%** of data was impacted each year. However, with the rise of ransomware, this paradigm has shifted, and organizations must accept that 100% of their data could be impacted in a single incident.

To successfully survive a ransomware attack, multiple best practices need to be implemented. In the following white paper, we will review the framework required to build a secure, resilient infrastructure that's designed for early threat detection, fast recovery and orchestration at-scale.

1. Data resiliency

When it comes to data protection, the industry-standard approach of the 3-2-1 Rule is something many organizations practice by default. While this was the gold standard for many years, it's no longer enough in the age of ransomware. Organizations need to go a step further and ensure they have an immutable copy of their data and completed comprehensive testing to ensure there are no errors in the data. Put another way, the new industry standard is the 3-2-1-1-0 Rule, a.k.a. the "zip code of availability".



Achieving the 3-2-1-1-0 Rule

Veeam uniquely offers a vast multitude of possibilities to achieve the 3-2-1-1-0 Rule, since every customer has different requirements and capabilities. For example, out of the box, **Veeam Backup & Replication** can adhere to this rule using the following setup. Three copies of the data exist (production workloads, a copy on the backup repository, and a copy on tape), on two different media (disk-backed repository and tape), one of which is offsite (tape), one of which is immutable (write once, read many tape media), and zero errors (proven with SureBackup).

Immutability for the data's lifecycle

Object storage is gaining popularity for many reasons: It's highly durable, cloud providers can offer it as a service and S3 Object Lock technology is an easy-to-implement way to achieve immutability. With support for writing backups direct to object storage, customers can leverage immutability throughout their data's lifecycle. Plus, by decoupling backup target management from the backup server's control plane, there is now an additional barrier of responsibility. With immutability enabled, even if a rogue backup administrator or threat actor does gain access to the backup server, your backups will still be safe.

Restore points can be automatically offloaded to a secondary location backed by immutable storage, whether that's on-premises or in the cloud. If long-term retention is required, Archive Tier supports immutability with Amazon S3 Glacier or Microsoft Azure Archive Blob Storage.

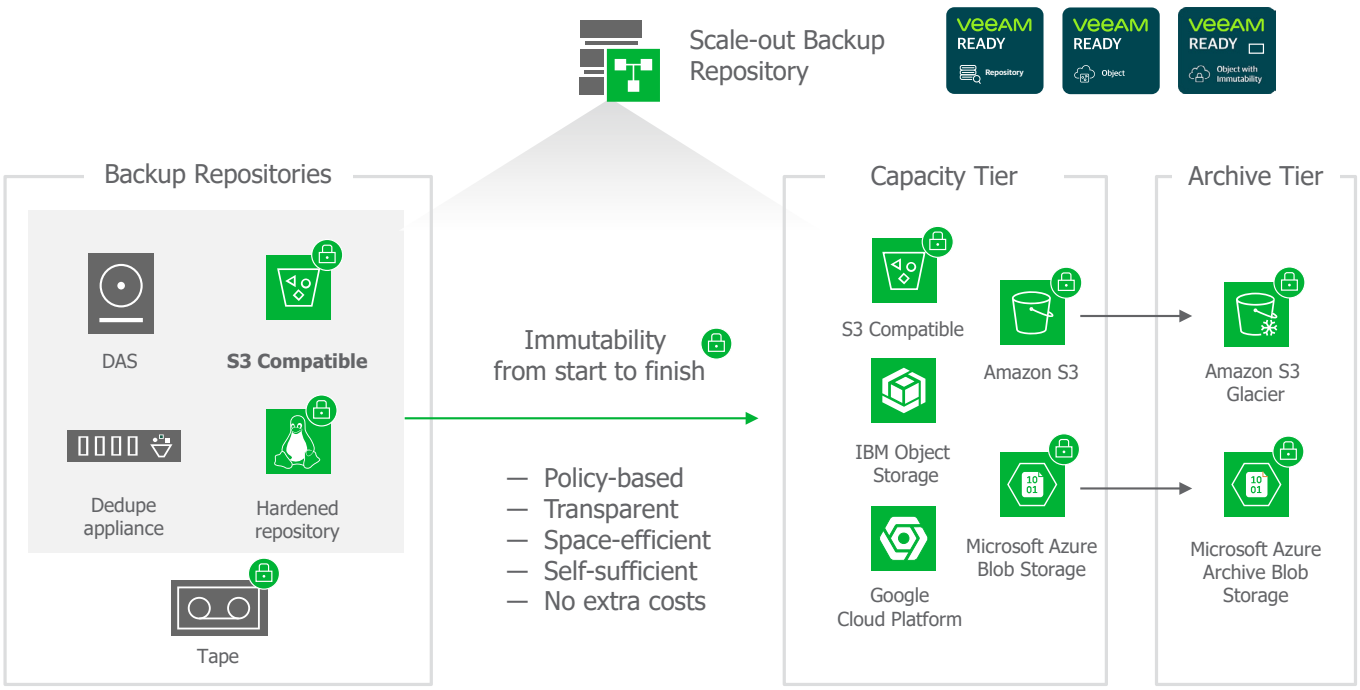
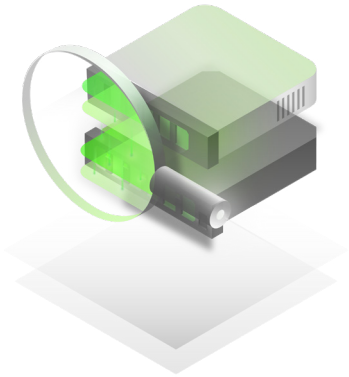


Figure 1 — Immutability throughout your data's lifecycle



If **Object Storage** is not available, then **Veeam's Hardened Repository** can also be leveraged. As part of its deployment, the Hardened Repository uses single-use credentials and native capabilities for Linux file systems to set the immutable attribute flag on backup files. As with any system, it is important to consider security requirements and best practices. Recommendations like limiting access (both physically and via network) and host hardening should be adhered to.

2. Design for *fast* recovery

During times of crisis, having backups is just the first step to recovery. Downtime for your business directly results in financial loss and damage to your brand. To get business operations back online as soon as possible, it is critical that you architect a resilient solution that can achieve this.

Veeam pioneered **Instant VM Recovery** in 2010 as a way to instantly get your VMs back up and running. Today, its use cases have grown to more than just VMs. Instant Recovery operations can be performed on Veeam Agent backups, including physical machines, Microsoft SQL Server and Oracle Databases, cloud-based workloads (i.e., Amazon EC2, Microsoft Azure and Google Compute Engine) and even NAS shares. Once the data is mounted and accessible, users can access their resources immediately. In the background, a migration can be performed to copy your data back to production. This will include the delta between your original backup and changes made as part of Instant Recovery.

Low RPO recovery from replicas

Veeam Data Platform's replication engine is another powerful tool and can offer finer granularity when it comes to achieving lower recovery point objectives (RPOs). While a backup job may run once every 24 hours, a replication job can be configured to run more frequently (e.g., every 2 hours). This can greatly reduce time between recovery points.

Replicas work by taking snapshots of the VM in question and replicating it to a designated landing zone, typically a DR site. The initial replication will be a complete copy of the VM, but subsequent ones will just contain the changes made since the last replication. To speed up the initial process, replicas can be seeded from backup files. Additionally, Veeam WAN Accelerator can be used to decrease replication time.

In situations where virtual workloads require near-zero data loss, **Veeam Continuous Data Protection (CDP)** can be used. By using VMware's vSphere API for IO (i.e., VAIO), replication can be measured in seconds while avoiding performance impact on the VM in question.

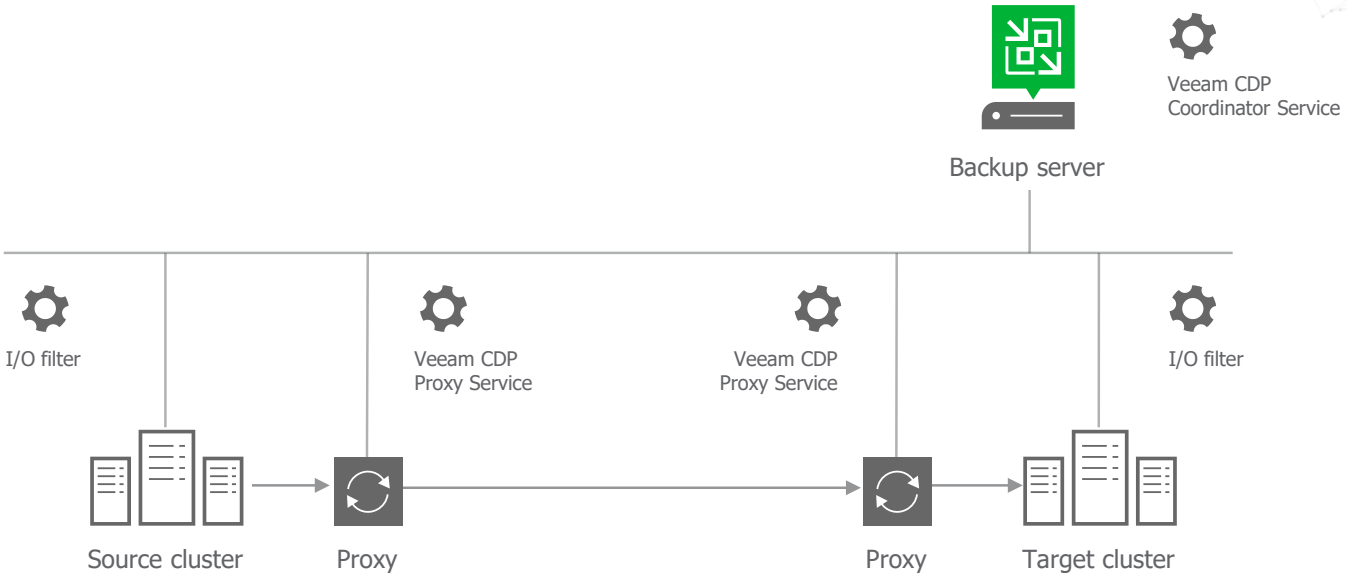
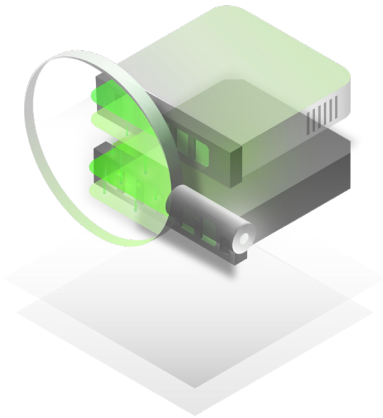


Figure 2 — Veeam CDP Architecture

Powerful Storage Snapshot integration



Veeam offers tight integration with many vendors and storage systems and provides Universal Storage API Integrated Systems. With this unique API, protecting and restoring data from snapshots is a straightforward task that does not require deep, subject-matter-expert level knowledge of storage arrays.

Backups can be performed through array-based snapshots to minimize impact on production. Additionally, **Veeam Explorer *for Storage Snapshots*** and **Instant VM Recovery *from Storage Snapshots*** provides users with the ability to quickly and easily perform recoveries ranging from entire VMs all the way down to individual files or application items. In addition to scheduling traditional backup jobs, snapshot orchestration ensures that you can meet your RPOs as well.

Trust but verify your backups

SureBackup is the Veeam technology that allows you to test backups and check if you can recover data from them. For example, if a threat is exposed on the next boot of a system, SureBackup could identify an issue that could prevent the system from booting or an application that will not start as expected. SureBackup jobs can ensure that applications will start as expected from backups (or replicas in VMware environments) and reporting will indicate that the restore point was indeed able to be restored. Testing is always recommended, but automated verification is even more critical when remediating ransomware threats.

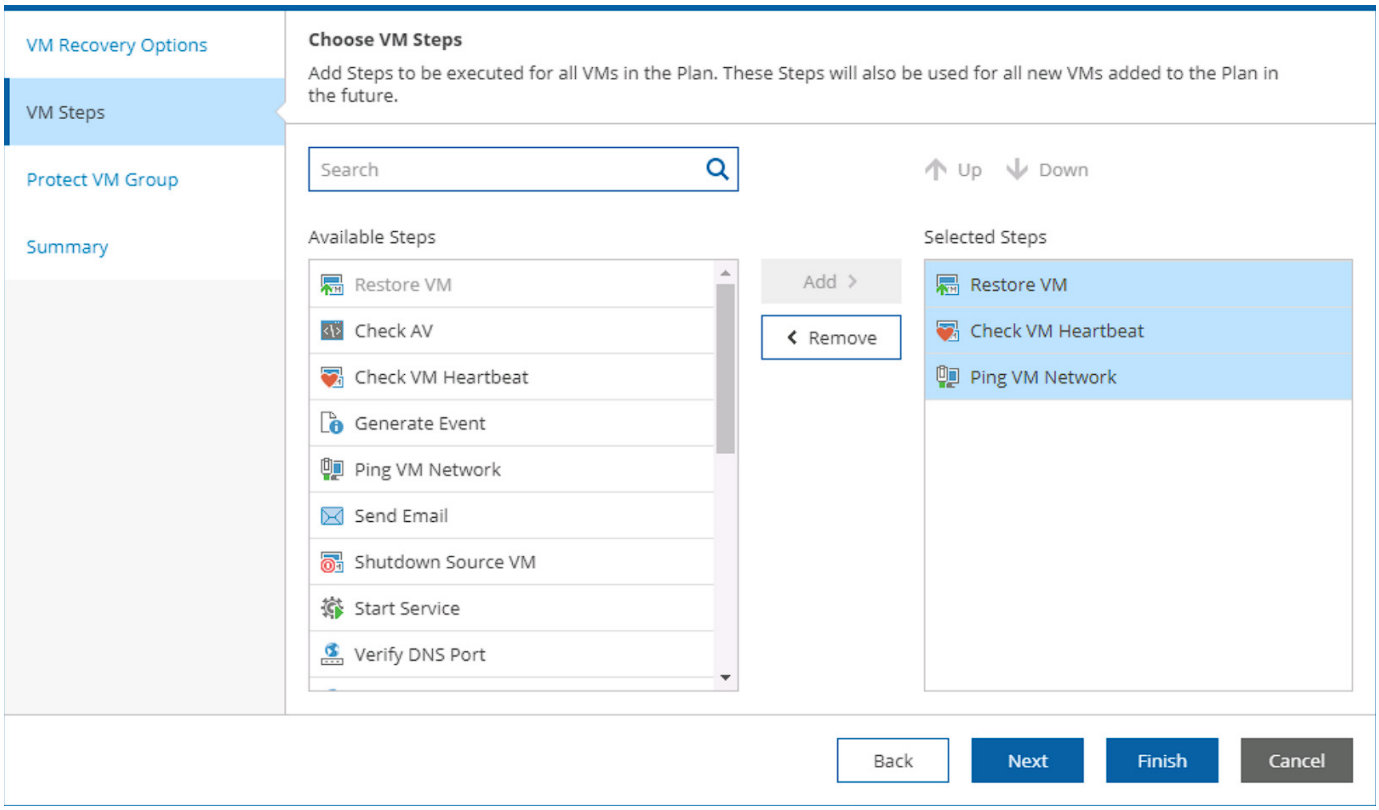
One of the more versatile aspects of a SureBackup job is the ability to leave your job running after it starts. By default, a SureBackup job will run and perform your configured checks. If your job is set to keep running, additional checks can be performed on the system from your backup restore point. This can include doing an automated or manual inspection to see if the ransomware threat is still present checking specific files for anomalies, data that's being encrypted or extracting selected data for further analysis.

Automate and orchestrate recovery

When ransomware does strike, rarely do we find ourselves performing just one restore. Commonly, many workloads are affected, and even workloads that are not directly attacked may still fail due to dependencies. When it comes to recovery at-scale, speed, automation and orchestration are imperative. Veeam Data Platform provides enterprises with the tools you need to recover quickly.

Any DR plan is only valuable if it works when needed. **Veeam Recovery Orchestrator** is able to provide proven results to give enterprises the confidence that they require. Customized dynamic documentation and reports provide the records and assurances that enterprises need when it comes to risk management. Similarly, after a plan is built, administrators can schedule automated tests to ensure their recovery will work as expected. To enhance security, automated testing enables administrators to scan restore points for ransomware, giving you peace of mind that the infection will not be re-introduced.

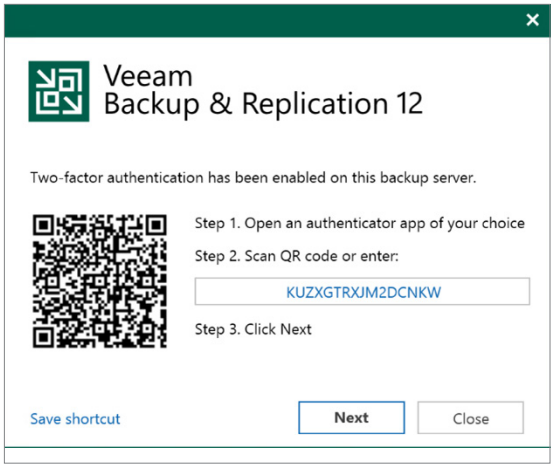
More commonly, enterprises cannot restore back to their production environments. Whether that's due to a lack of resources, forensic investigations or cyber insurance requirements, without somewhere to restore to, recovery cannot be achieved. Veeam Data Platform can provide the versatility that enterprises demand by orchestrating recoveries directly into Microsoft Azure.



3. Apply multi-layered security

Any security professional will tell you that the first step towards security is to lock the front door. Whether that be a physical front door or a metaphorical one, a defense-in-depth strategy should be used. Veeam provides an array of tools that enterprises can use to help them raise their shields against malicious threat actors.

Keep attackers out



Multi-factor Authentication (MFA) should be enabled wherever possible. From an OS perspective, infrastructure components like proxies, repositories and the backup server itself should require some form of MFA to log on. Additionally, MFA should be enabled for users who require access to the Veeam Backup & Replication console. This feature will also work in offline mode should the backup server not have access to the internet. This provides increased flexibility with security by design.

When interacting with guest OSes, like a Windows Server running SQL Server, tools like group Managed Service Accounts (gMSA) are a perfect fit. These accounts use random, auto-generated 240-byte passwords that automatically change every 30 days. Holistically, this provides an extremely strong and trusted interface to interact with workloads.

To review your current security posture within your backup environment, you can run the **Security Best Practices Analyzer** at any time. This tool will provide a summary of security best practices as it relates to the Veeam Backup & Replication server's configuration. As changes to the environment are made, the tool can be run to review the impact.

Protect data in-flight and at rest

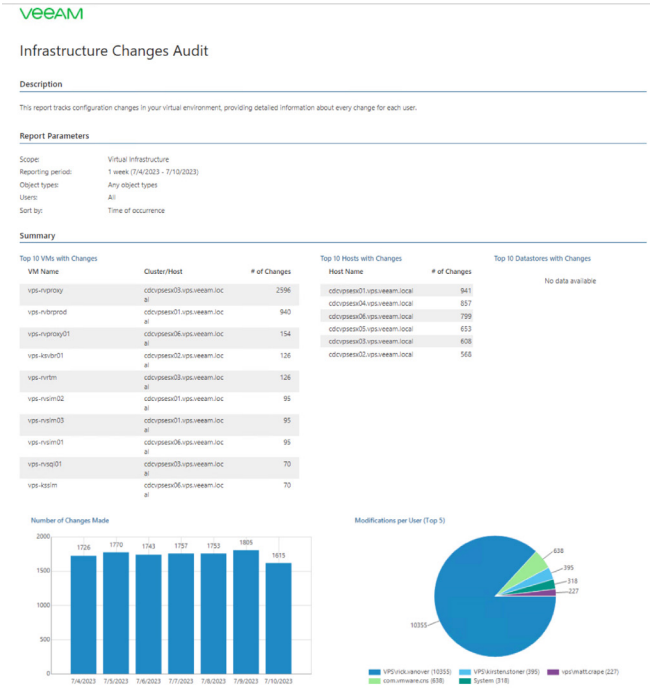
Regardless of your backup data's location, encryption should be a consideration. Although immutability is critical to prevent malicious attackers from deleting your backups, this does not necessarily prevent that same data from being copied and exfiltrated.

The encryption technology in Veeam Backup & Replication allows the product to protect data both while in transit between backup components and at rest, stored at its final destination. Customers can use one encryption method, or a combination of both, to protect against unauthorized access to important data through all the steps in the data protection process.

4. Monitor for emerging threats

Veeam ONE is a key component of Veeam Data Platform since it's primarily responsible for providing proactive monitoring and analytics. Almost all attacks have pre-cursors that can be identified, and being alerted to these and acting upon them can make the difference between winning or losing a battle against ransomware.

Identify unsanctioned access and changes



Commonly, attackers often leave markers in your environment. For example, when credentials are stolen attackers may start logging into various workloads on the network. This allows them to verify that their stolen credentials are valid and test what permissions they have and on what systems.

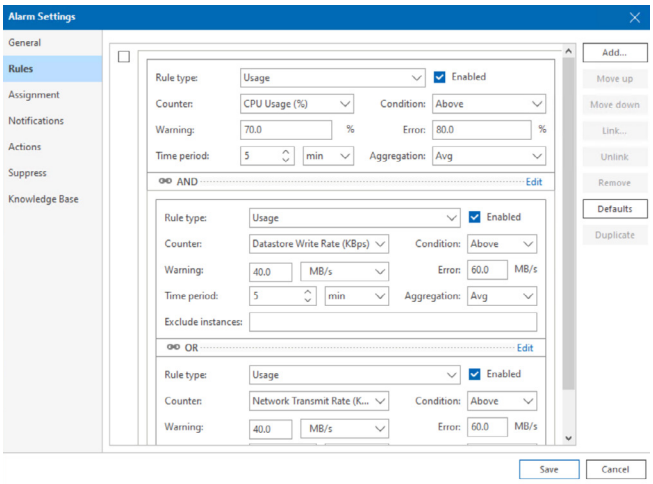
The Infrastructure Changes Audit report should be run and reviewed regularly since it can help identify changes within your virtual environment. Changes can be tracked against VMs, hosts and datastores while providing details like how many changes have occurred, what changes occurred, who performed the actions and when. This can quickly identify unsanctioned behavior that can be halted.

Uncover changes in backup sizes

One of the key characteristics of ransomware is its mission: Encrypting files. This means that new data is created, and that it may be backed up. Although this is far from ideal, this does provide another data point to monitor: Backup file sizes.

The **Suspicious Incremental Backup Size** alarm can be configured to monitor for drastic changes to incremental backup file sizes. Alarms can also be highly configurable to include tasks such as sending alerts via email, running pre-defined scripts to perform tasks or collect information, or even starting a SureBackup job.

Identifying possible threats in real-time



Encryption is a CPU- and disk I/O-intensive operation, which results in a new encrypted file being created. As such, telltale signs of an active ransomware attack can be detected by monitoring for spikes in metrics including CPU usage, disk write rates and network transmit rates. With Veeam ONE, the **Possible Ransomware Activity alarm** can be enabled and fine-tuned to trigger based on these observations.

When it comes to Veeam ONE alarms, a recommended practice is to duplicate that alarm and fine-tune it for your environment. Using this alarm as an example, you may find that you have some database workloads that typically run on the higher side when it comes to CPU usage. A copy of the alarm can be used to tweak the values and only apply those thresholds to a specific scope.

5. Automate documentation, security and testing

Despite being critical, keeping DR plans up to date is a challenge that affects enterprises of all sizes. No IT department wants to be in a situation where a DR plan is executed just to find out that the documentation is out of date, missing steps or even completely wrong. Veeam Recovery Orchestrator overcomes this challenge by automating the process of creating documentation for each orchestration plan that you create.

Plan Steps & Default Parameters

Restore VM

Parameter	Description	Default Value
Description	This is a default step for every machine added to a Restore Plan. It restores machines from backup files into the specified recovery location.	None
Test Action	This step will always be executed in a Test DataLab environment only.	Execute
Critical Step	Choose Yes or No to define whether this step is critical to the VM recovery. If critical step, then failure will cause the VM to be marked as failed	Yes
Restore Timeout (minutes)	Timeout (in minutes) for the restore process. As soon as this timeout expires, Orchestrator will stop both the restore process and all the restore tasks currently running on the Veeam Backup & Replication server. If you set the parameter value to 0, the timeout will be disabled, but you will still be able to interrupt the restore process by halting the plan. This setting applies to Recovery, Migrate and Rename step independently.	0
Retries	Number of retries to perform in case the step fails on the first try.	2
Restored VM Name	A name for the newly created VM	%source_machine_name%

Check license and availability

Parameter	Description	Default Value
Description	This step checks whether Orchestrator is licensed to recover this system as a VM. If not, the check displays the ordinal number of the VM in the license queue.	None
Critical Step	Choose Yes or No to define whether this step is critical to the VM recovery. If critical step, then failure will cause the VM to be marked as failed	Yes
Timeout	Timeout (in seconds) for the step	300
Retries	Number of retries to perform in case the step fails on the first try.	1
Failback & Undo Failover Action	Choose Execute or Skip to define whether this step is executed during Undo Failover and Failback operations.	Execute
Test Action	Choose Execute or Skip to define whether this step is executed during plan testing in DataLab	Execute

The documentation is human-readable, easy to follow and can be generated whenever required, like after a change has been made.

Securely restore your data

When a ransomware attack does occur, backups are your last line of defense. Unfortunately, malware commonly has a dwell time in your environment. This is a period of time where it just sits there, waiting to be activated. Because of this, your backups might unknowingly contain a copy of the threat. Thus, there's a risk that restoring your backups will just reintroduce threats back to the environment.

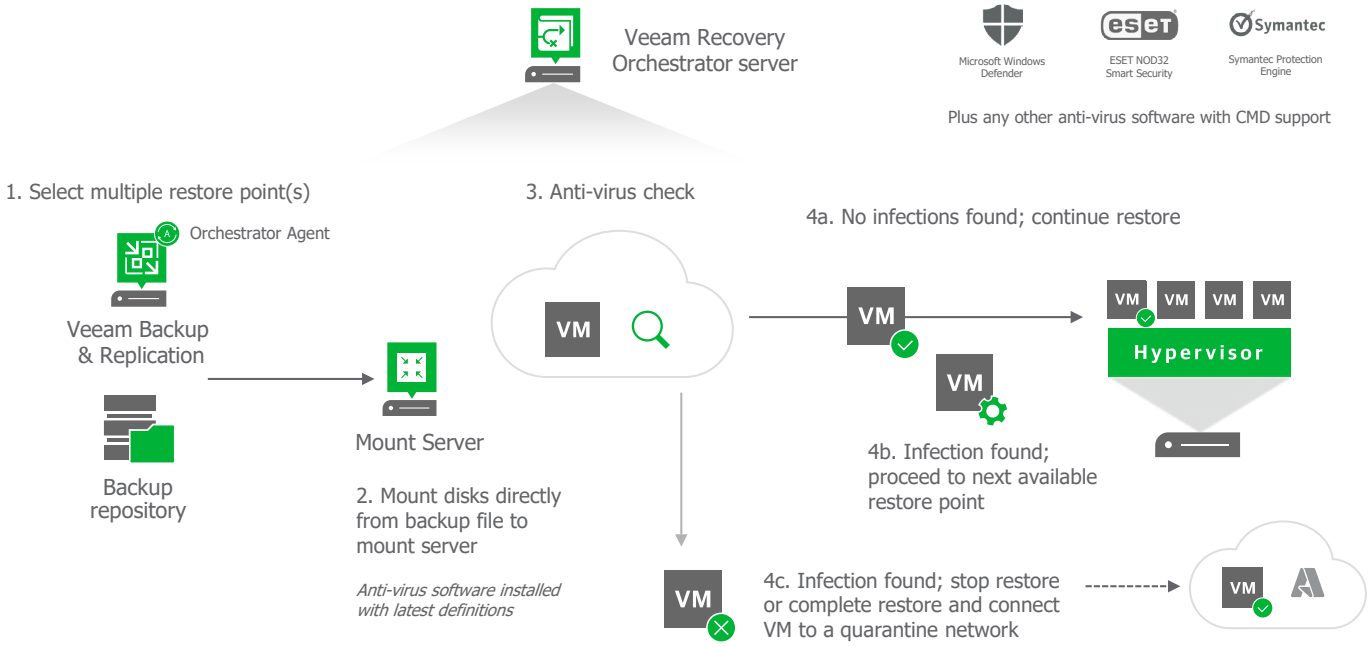
Veeam Backup & Replication's **Secure Restore** is the answer to this threat. Secure Restore can be leveraged to perform a malware scan as part of the recovery process. Machine disks from the backups are mounted to a mount server which then performs the scan. If no threats are detected, then the restore continues as normal. If malware is detected, however, users can choose whether to abort the restore or continue with restrictions (i.e., disable the network interface).

Clean DR at scale

What about when disaster strikes, and entire data centers are affected? Veeam Recovery Orchestrator's **Clean DR** provides users with the ability to perform safe and orchestrated recoveries at scale. Similar to Secure Restore in Veeam Backup & Replication, which is the base for Clean DR, disks are automatically mounted and a malware detection scan is performed. If no threat is found, then the restore operation can continue as per the recovery plan.

If a threat is found, administrators can perform one of the following actions:

- Scan the next newest restore point for malware
- Stop the restore
- Complete the restore with the suspect restore point and connect your VM to a quarantined network



When it comes to malware detection engines, customers have the option to use one of the many integrations that exist today, or they can add their own by creating and customizing an XML configuration file. More details can be found in Veeam KB 3132.

Prove your DR plan's compliance

Testing DR plans is something that many organizations cannot achieve despite their desire to, even while knowing that it should be performed. Automated and scheduled testing with Veeam Recovery Orchestrator streamlines the entire process of testing by leveraging Veeam **DataLabs**.

RPO

Result	Check	Details
[i] Info	RPO	Target RPO is 24:00 (HH:mm)
✓ Success	Target RPO Met	Yes
✓ Success	VMs not meeting RPO	None
✓ Success	Worst RPO failure	None

RTO

Result	Check	Details
[i] Info	RTO	Target RTO is 01:00 (HH:mm)
[i] Info	Duration	Test duration was 00:04:56 (HH:mm:ss)
✓ Success	Target RTO Met	RTO achieved

DataLabs uniquely enables Veeam Data Platform backups of both Agent-based and virtual workloads to be fully restored into a sandboxed environment. As such, when a DR test is performed, the entire plan is carried out with an out-of-band network. This not only ensures that your plan will work as expected, but it also provides you with real-world RPOs and recovery time objectives (RTOs) that you can use to prove your compliance.

6. Use API-driven threat detection

When it comes to threat detection, a common challenge that enterprises face is the impact of performing a resource-intensive detection scan on production workloads. Scanning files for threats or looking for known artifacts and threat indicators can lead to excessive CPU usage and degraded disk performance. These penalties can be avoided while still giving you the ability to scan for threats with an offline scan against your backups.

No-impact threat hunting

First introduced in Veeam Backup & Replication v10, the Veeam **Data Integration API** provides customers with unbridled access to their data in an offline fashion. This capability allows backup file data to be exposed as a mounted folder and allows access to data that is available in backups created by Veeam Backup & Replication. This capability is an excellent technique to ensure that ransomware or other threats won't be restored into production. The API also allows data to be scanned on a regular basis for additional threats and can allow security teams to perform threat hunting activities in an isolated, secure environment.

Additionally, since data is mounted as a file system and not an actively running system, threats cannot be executed and/or loaded into system memory. This provides a safe and effective way to perform forensic-like audits and searches while minimizing impact and removing threats to other workloads.

Identifying non-compliant data and changes

Similar challenges exist when it comes to classifying data on these systems and ensuring that regulatory compliance is being adhered to. Performing checks on file content and modification is not something that can be performed in production, but it is something many organizations would benefit from. Since the Veeam Data Integration API leverages **PowerShell**, enterprises can develop code to perform the tasks that they require. These tasks include identifying where Personally Identifiable Information (PII) resides or determining if sensitive files are changed.

By performing these analytics and recording these results, organizations are empowered to track the systems their data resides on with confidence. As a benefit, customers can use this data to build and review restore plans with the added benefit of ensuring data locality and compliance ahead of time, and not during a disaster.

7. Plan for an inaccessible data center

Having a location to restore your workloads back to is a critical task that needs to be planned ahead of time. Whether your production servers are offline due to a forensic investigation, or you don't have the resources available to restore back to your data center, enterprises need to ensure that they are back online as fast as possible.

Veeam Recovery Orchestrator, which is part of Veeam Data Platform — Premium edition, empowers customers to build automation and orchestration plans, granting them the ability and flexibility to get workloads up and running while ensuring that their SLAs are met.

Recovery outside your data center

One of the key differentiators that Veeam Recovery Orchestrator has to offer is the ability to restore VMware workloads and Veeam Agent backups directly to Microsoft Azure in addition to VMware environments. Enterprises can plan for recoverability by creating orchestration plans to combat downtime, whether that's due to ransomware or aftereffects like restrictions imposed by law enforcement. Once plans are built out, they can be tested in a sandboxed environment. This not only ensures that everything will work as expected, but it will also provide proven RPOs and RTOs, giving you the confidence that you need to recover from an incident.

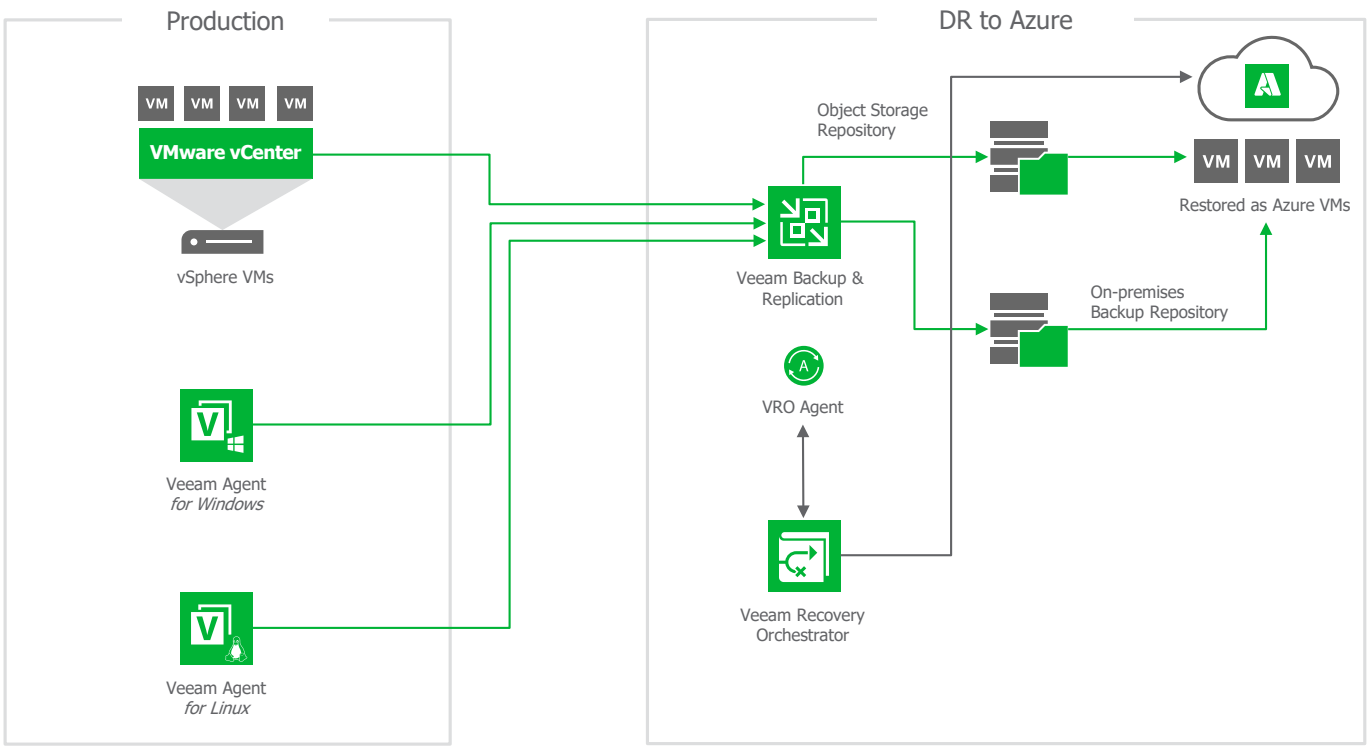


Figure 9 — Orchestrated recovery to Microsoft Azure

Summary: Ensuring rapid ransomware recovery

Ransomware attacks have been increasing at an alarming rate and causing significant damage to businesses and organizations. These attacks target critical data and render it inaccessible to owners until a ransom is paid. In many cases, even after payment, this data is not restored and perpetrators continue to hold it hostage. The best way to protect against ransomware is to have a solid backup plan in place.

Trusted backups are crucial to surviving ransomware attacks. Organizations need confidence in their ability to quickly recover from an attack of any size. It is imperative that companies continue to bring backup and recovery into their overall security program to ensure that data is resilient and protected.

Building a comprehensive security program requires the merging of people, processes and technology in ways that focus on continuous improvement that allow organizations to move from a reactionary defense to a proactive posture. No matter the methodology companies choose, there must be measurable outcomes that allow IT teams to defend against attacks and recover quickly when an attack is successful.

The goal of a ransomware recovery plan is to minimize downtime in the event of a ransomware attack and automate the process to reduce risk. Before an attack happens, organizations need to be sure they are equipped with the most complete set of capabilities on the market to counter any potential threat.

By following these steps, executives can ensure that their organization is well-prepared to respond to a ransomware attack and can quickly recover without paying a ransom. While there is no foolproof way to prevent ransomware attacks, having a clear understanding of best practices to protect data and the steps involved in successful ransomware recovery will allow you to reduce the attack surface while gaining visibility into emerging threats. The result is a response team who are better equipped with the knowledge and tools they need to defend their data and protect their business from the threat of ransomware.

Data Protection Trends Report 2023

Ransomware Trends Report 2023

Watch 6 Short Demos to Overcome Ransomware


VEEAM