5 Ransomware Protection Best Practices

Veeam's definitive guide to data protection

Rick Vanover

Senior Director,
Product Strategy, Veeam Software

Edwin Weijdema

Global Technologist,
Product Strategy, Veeam Software

Contents

Introduction and who should read this paper

The war against ransomware is real and everyone must be prepared for an attack on their data. The good news is that by preparing in advance, you can align to a framework that provides a reliable strategy when status quo operations are disrupted.

The technical advice in this paper will provide actionable recommendations to backup administrators and site reliability engineers (SRE), plus technology and operations management professionals. However, the backup team is just the start! The reality is that everyone must take a security-focused approach to protecting the critical data within an organization with these five best practices: identify, protect, detect, respond and recover.

This content will highlight the capabilities provided by Veeam® and the practical advice of two authors: Rick Vanover, senior director of product strategy at Veeam, and Edwin Weijdema global technologist of product strategy at Veeam. This paper is a guide to help you start the journey to building higher resiliency and recoverability of your critical data. This is achieved by aggregating expertise from all possible angles, including external advice.

There are ever-increasing threats to your data, so every step you take to prepare now, will provide you with options when the time to respond comes. Start the journey now and take action on this urgent matter. We'll show you the way!

Ransomware 101

How do cybercriminals get YOUR data?

Thinking you don't have any valuable data is the most common mistake we hear from our users. When you move through the digital world, you leave digital traces behind like digital breadcrumbs and cookies. When you register at a website with a username and password, often that username is your email address and the password is, for 60% of people, a re-used password.

Cybercriminals hack websites and harvest login information like email addresses, login names, domain names and any other information they can retrieve. This is just the first piece in a larger, more elaborate digital puzzle for cybercriminals. The data they retrieve will be placed in cloud caches, and then analyzed and enriched with other data sources like a social media post or something similar. These puzzle pieces can be glued together with the extra metadata extracted from those social media posts.

As soon as cybercriminals can establish relationships between the different data puzzle pieces they analyzed, they create a profile and you become a target. These digital profiles give cybercriminals new keys and opportunities to gain access to newer, larger and more sensitive data sources.

Data is the lifeblood of any modern organization. For most organizations, if something contaminates or stops the flow of data, they are instantly paralyzed. So, data is extremely valuable, which means its great ammunition for cybercriminals. They use ransomware attacks to hold your most important and valuable assets for ransom and lock you out at the same time — while making sure no copies are available for restore!

"Know that most cybercriminals target data, and they get that data by hijacking accounts like yours!"

Through the eyes of a threat actor:

As a threat actor, I lurk in the shadows and patiently observe you to identify which systems are in use, if multiple environments are used, who's using them and where potential access points are. The easiest way for me to enter your organization is if I can get help from the inside, by gaining unmarked, legitimate and active access credentials. To do this, I identify potential human targets that can supply me with a door to those access credentials, without actually needing to know the credentials themselves.

After I identify potential entry points, I start off with a (spear) phishing attack, because I just need one person in the organization to click that link and let my malware in. As soon as the malware feels comfortable and settled, I'm notified on my cloud-based webserver that remote access was successfully established.

Then, it's time to use my fingerprinting tools to uncover hidden vulnerabilities, unpatched systems and open ports. Before I move forward, I'll protect my access by setting up a redundant and highly available base of operations.

At this point, it's too early in the process to make myself known, so I have to remain in stealth mode for now. I use my administrative console to quietly observe your online activity and plan my next course of action. After a few weeks or months of incubation (i.e., dwell time), it's now safe to continue my journey. Now I'll go for high-value targets, like highly privileged accounts, organizational data caches and backup repositories.

Before you detect me, I will make sure to use orchestration and automation techniques to deploy the necessary tools, ransomware and management agents to all the machines at my disposal. This way I can respond quickly and at the right moment to fulfill my plan. Then, I will remove or disable your AV measures, routines will be altered, important documents will be deleted or blanked and backups will be purged or encrypted.

Now I'll wait for an opportunity where I'm least likely to be discovered, often a Friday evening or a long weekend. I'll need the encryption process to execute this thoroughly and without interruption.

I now hold the encryption key that controls whether or not you can recover from this ransomware attack. If I did my job successfully, I've removed any timely recovery possibilities to restore your operations to normal. But don't be sad! Your data isn't lost! I'll make sure the payment process and speedy recovery of your data is as smooth as possible. I'll even give you samples of your files on request as proof. It's not personal, it's just business (Including Ransomware as a Service)!

Ransomware history

An important precondition for the emergence of ransomware was the introduction of the IBM Personal Computer (PC) with Microsoft's MS-DOS operating system in 1981. The IBM PC revolutionized business computing by becoming the first PC to gain worldwide adoption.

The first ever documented malware extortion attack was delivered through the distribution of 20,000 floppy disks to attendees of the World Health Organization's AIDS conference in 1989. It claimed to contain a program that analyzed an individual's risk of getting AIDS with a questionnaire.

These floppy disks also contained malware that would count the number of PC starts taken until it had reached 90 starts and activated its payload. The malware would hide the directories and encrypt the names of files on the C:\ drive. To regain access, users would need to send a check of $189 to PC Cyborg Corporation at a P.O. Box in Panama. Malware was used to extort users to regain access to their data by paying a ransom. Thus, ransomware was born!

The invention of the internet increased the potential of ransomware even further by reach, impact and possible gain for cybercriminals.

- Reach: more and more connected users and devices were discoverable through the internet
- Impact: data is the lifeblood of every modern organization nowadays. So, stopping the flow or contaminating that data can instantly paralyze an organization
- Gains: the value and volume of data has skyrocketed the last couple of years

The last but most important contributor to the rise of ransomware is the invention of cryptocurrency. Cryptocurrency built on blockchain technology and enables a form of digital cash that can be sent peer-to-peer without needing a central bank or authority to operate and maintain the ledger. In this way, cryptocurrency is much like physical cash.

Cryptocurrency gained enormous popularity with cybercriminals due to the privacy and anonymity that cryptocurrency networks offer. This allows users to keep their identities and transactions confidential.

All of the factors mentioned above are fueling a rapidly growing criminal enterprise.

Ransomware behaviors and evolution

Current ransomware strains operate in several different modes, and it is expected that these modes will continue to evolve. Current threats can simply encrypt data and demand payment, or, increasingly, act by deleting data or extortion regarding the leaking or selling of the data. There have also been threat actors that work at the infrastructure or application level, like databases and file systems.

At Veeam, we have adopted a mindset that addresses the moment that ransomware response is needed. Despite all the education and implementation techniques that are employed to combat ransomware, organizations should be prepared to remediate a threat if introduced. At Veeam we have devised an approach towards remediating ransomware. This approach contains these two recommendations:

- **Do not pay the ransom**
- **Restoring data is your only option**

With the recommendations outlined later in this document, organizations should be prepared to have layers of resiliency to defend against when (not if) a ransomware incident occurs.

Market observations on ransomware

Veeam has a large global customer base and regularly conducts surveys and enhances their products to address the threat of ransomware. From our most recent customer survey, a few noteworthy statistics can be shared to help indicate the pulse of the industry in regard to ransomware behavior in the market at-large.

Observation 1: ransomware source

Consistent with other industry reporting mechanisms, the Veeam survey of organizations who have had ransomware incidents showed that the top modes of ransomware entry include:

- Phishing emails
- Remote access
- Exploited vulnerabilities

Observation 2: post-ransomware incident changes

It's always helpful to identify what organizations do after a ransomware incident to prevent that type of situation from occurring again. The Veeam survey identified the following post-incident changes as being the most common:

- Bolstering backup and recovery options
- Investing in end-user education
- Security-related internet access changes
- Having orchestration and automation in place to aid response and recovery
- Investing in detection technologies

Specific infrastructure changes like isolation, explicit access, minimal permissions and similar security tips for the infrastructure components that are the most critical to the recovery process are very important. Many organizations who have recovered from ransomware incidents have implemented specific management fabrics for their backup infrastructure to provide an additional layer of separation with no connectivity to other systems and resources.

Observation 3: ultra-resilient media is key

The recent survey indicates that organizations are implementing backup and recovery solutions that leverage ultra-resilient media. These are media types that are either offline, air-gapped or immutable. Having one or more copies of backup data with one (or more) of these characteristics is critical to a successful recovery from ransomware. Ultra-resilient media options include:

- Immutable backups in AWS Amazon S3 and S3-Compatable storage systems
- Immutable backups in Linux with the hardened repository
- Tape media that's removed from the library or marked as WORM (Write Once Read Many)
- Veeam Cloud Connect with insider protection
- Offline (i.e., ejected) removable media or rotating drives

We are now seeing that organizations are retaining more backup copies and incorporating more ultra-resilient options. Combined, these two behaviors pave the way for robust recovery from data loss that's caused by ransomware.

NIST cybersecurity framework: 5 best practices

Veeam collaborates closely with standard bodies and brings deep expertise and experience that comes from the government security sector. Combining these experiences and linking them to the right functions in a framework allows people at all levels and disciplines within an organization to develop a shared understanding of cybersecurity risk. Veeam has opted to use the NIST cybersecurity framework (NIST CSF) because it's used worldwide as an excellent starting point for cybersecurity management and includes common terminology across all involved stakeholders.

Drafted by the National Institute of Standards and Technology (NIST), this cybersecurity framework provides a uniform set of rules, guidelines and standards for organizations of all sizes and all industries. This cybersecurity framework can provide value as a top-level security management tool that can help assess cybersecurity risks in your organization.

The NIST CSF is voluntary guidance, based on existing standards, guidelines and practices, that is meant to help organizations to better manage and reduce their cybersecurity risk. In addition to helping organizations manage and reduce risks, the framework was designed to foster risk and cybersecurity management communications among both internal and external organizational stakeholders. Creating a common language allows people at all levels and disciplines within an organization to develop a shared understanding of their cybersecurity risks.

The NIST CSF and its five functions — identify, protect, detect, respond and recover — is widely considered to be the default standard for building a robust cybersecurity program. The NIST CSF can be helpful whether you're just getting started in establishing a cybersecurity program or if you're already running a mature program.

In this paper, the five functions of the NIST CSF will be looked at from two key perspectives. The first perspective is the defense perspective, which looks through the eyes of a cybersecurity specialist that has cybersecurity best practices to follow. The second perspective is the opportunity perspective, which looks though Veeam, which has specific features and solutions that can help increase your digital resilience according to the five NIST functions.

Identify

The NIST identify function lays the groundwork for cybersecurity-related actions that your organization can take moving forward. Determining what environments exist, what risks are associated with those environments, and how this all relates in context with your business goals is crucial to finding success with the framework.

"The question you should ask yourself is: what processes and assets exist; what risks are associated with them and how does that relate to my business goals?"

Cybersecurity best practices for identification

One of the first things any battle will teach you is that you can get to know your enemy by learning to think like them. You have to think about what cybercriminals are looking for and how they plan to achieve their goal. To do this, it's crucial that you have full visibility of your people, processes and technology.

Know what you have, where you have it and the value is of every single resource individually plus the value all resources combined. Cybersecurity experts developed a set of best practices over the years to beat ransomware. These best practices include the basic tenet that cybersecurity is a life-cycle process — it's a journey.

Important best practices for the identify function are:

Tip #1: The human firewall/probing

Technology alone can't strengthen your organization's cybersecurity posture. Amid the growing complexity and threat of cyberattacks, organizations must focus on building a multi-layered defense. This means that everyone must be aware of security risks and potential incidents and report anything suspicious. The importance of this human layer of protection lies in the fact that many breaches are due to employee error. Successful hacks are often caused by carelessness, simple mistakes or lack of knowledge of cyber threats and cybercriminals' practices.

Knowing that phishing, remote access (RDP) and software updates are the three main mechanisms for entry by a cybercriminal is a huge help in focusing the scope of where you want to invest the most effort from an attack vector perspective.

How cyber-aware is your workforce?

Identify potential knowledge gaps within your workforce by running a cybersecurity awareness program. Evaluate your organization's cybersecurity awareness maturity level by, for example, using a phishing simulation program to uncover the current level of cyber awareness.

Have you ever received an email asking you to click on a link to check the status of a package that you didn't remember sending? Or one that asks you to click a link to confirm your password for an account? These both could have been — and likely were — phishing emails.

A human firewall is an important layer in the defense against ransomware of any type. By working together, we can identify threats, prevent data breaches and mitigate damage. The more employees you have committed to being part of the human firewall, the stronger it gets!

Tip #2: Have an always available and up-to-date business continuity plan (BCP)

Which processes are crucial for your organization? Who do you need to contact in case of a business-disruptive event? Making sure that your business continuity plan (BCP) is always available, even if everything is lost and locked down, is crucial for an organization's survival. The best practice is to make sure that your BCP is stored in a separate location, is immutable and is available 24/7/365. A BCP should outline how a business will continue operating during an unplanned service disruption. Manual workarounds should be outlined in the BCP so that operations can continue until digital systems and services can be restored.

Tip #3: Tagging your digital assets

Insight into which assets are critical to your organization and how to effectively protect them is vital in creating a successful cybersecurity response plan. Before you start protecting, you should identify and tag these assets to make the most effective plan. Tagging digital assets can mean the difference between having to look for a needle in a haystack and finding the specific asset you need with a simple search.

Veeam opportunities for identification

You have unique opportunities to identify your data of interest with Veeam. These opportunities are as follows:

Data tagging: tagging your virtual machines (VMs) paves the way for good organizational constructs in the data center. Ideally, all new VMs would be created with a tag that describes its data protection strategy. This can include simple levels like backup only, but you can also allow tags to be subject to disaster recovery (DR) or additional protection. It's also possible that you'll have workloads tagged with a "nobackup" tag as part of an intentional decision to not protect certain workloads. The goal here is to have the protection status of all workloads identified in tags from the start, and the tagging process can be used for other business reasons (like being in-scope of a compliance requirement). This can feed into the other functions of the framework, namely the **protect function**, to build backup and replication jobs through tags in Veeam Backup & Replication™.

Data locality: Having location assignments applied to workloads, backup storage and more can allow organizations to have location control of their data. In Veeam Backup & Replication, core components of the infrastructure can have locations assigned to them to provide visibility to where your data is and where it may be backed up and/or restored to. This can enable better control and visibility when needed in the **respond** and **recover** functions of the framework.

Business view: Veeam ONE™ provides a business view, which is an excellent way to use categories and groups for visibility in terms of business stakeholders by labeling the technology assets assigned to them. Business view groups can be synchronized with vSphere and Hyper-V tags. This can synchronize the creation of tags based on Veeam ONE categorization, which improves visibility and manageability.

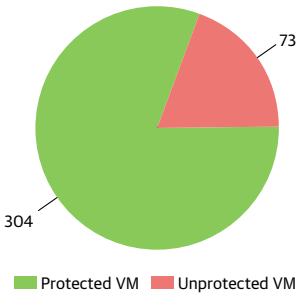
Protected VMs and computer reports: This Veeam ONE report provides users with a great view of what is and is not being backed up within assessed environments. The VM that has no backup alarm can be used in conjunction with Veeam ONE remediation actions to automatically add systems that are not being backed up to a backup job. The figure below shows the protected VMs report, which identifies what is and what isn't being backed up. Note that subsequent pages of reports like this will list the individual systems that are and are not backed up.

Summary

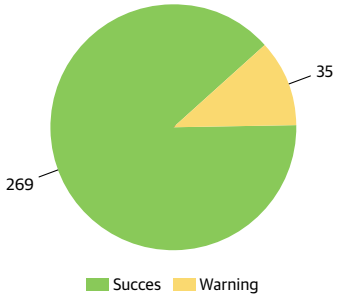
VMs Overview

Total VMs:	388
Including VM Replicas:	11
Protected VMs:	304
With Backup:	303
With Replication:	1
Unprotected VMs:	73

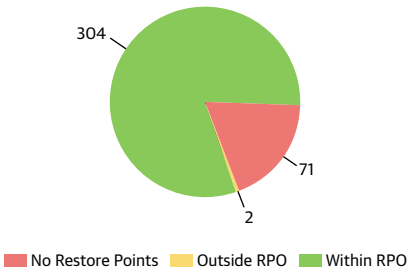
Protected VMs



VM Last Backup State



VM Last Backup Age



Protect

The protect function is essential because it helps develop and implement appropriate safeguards to ensure critical infrastructure service delivery. It proactively supports your ability to limit or contain the impact of a potential cybersecurity event.

"The question you should ask yourself is: what appropriate safeguards should we implement to ensure the protection of our organization's assets?"

Cybersecurity best practices for protection

Successfully protecting your organization against ransomware is all about understanding current attack vectors: From what threats and adversaries are you protecting your digital systems/services? If you know what you're protecting against, it becomes easier to take the correct countermeasures. The best practices for protection are:

Tip #4: The human firewall — education

Educating and training your staff around cybersecurity is a highly effective and efficient way to raise your protection level against ransomware attacks. Your organization is not full of security experts, so you need to provide basic knowledge and delineate the appropriate actions to take when faced with an incident. You also need to repeatedly test the effectiveness of your cybersecurity training programs.

Many organizations only have security awareness training once a year, but this is unfortunately not enough. Human firewall training should be continuous, with employees receiving updates and new briefings as threats arise. People should also all be educated on new issues whenever they change job titles. That cybersecurity muscle memory should be trained before a potential security incident. Remember: an informed workforce is your greatest defense and protection measure against ransomware.

Tip #5: The 3-2-1 data protection rule

The 3-2-1 Rule is an industry standard for how to protect data and it's your ultimate line of defense in the fight against ransomware. This rule asks you to make sure you keep at least three copies of each piece of important data, store your backup data on two different media types and replicate one copy of your data off-site.

Tip #6: Secure by design

Adding security to an existing infrastructure is much harder and more expensive than just thinking about it enhancing an existing infrastructure while you're designing a new or refreshed infrastructure. In a virtual infrastructure, it's good practice to build a master image that's secured from the start. Removing all known attack vectors and only opening access when components are added and need specific openings or extra software to function properly, is a best practice. This way, all builds are consistent and kept up to date, which creates a secure baseline.

Tip #7: Keep it simple and straightforward principle (i.e., K.I.S.S.)

Overly complex designs become harder for IT teams to manage, which makes it easier for an attacker to exploit weaknesses and stay in the shadows. Simpler designs that are easy to keep track of are fundamentally more secure. Use the K.I.S.S. (keep it simple and straightforward) principle for your designs.

Tip #8: Principle of least privilege

This principle means only giving a user account or process the privileges that are absolutely essential to perform its intended function. The principle of least privilege is widely recognized as an important design consideration that enhances the protection of data and functionality from faults and malicious behavior.

Tip #9: Segmentation

Ultimately, all security is about protecting a valuable asset. In this case it's data, but that protection involves an in-depth defense strategy that includes all layers. To do a defense-in-depth strategy, you should identify your most valuable data and build layers of defense around it to protect its availability, integrity and confidentiality. Segmentation means dividing your infrastructure into zones where you group objects into logical zones by looking at the level of access needed, common restriction policies restrictions and connectivity both in and out of that zone.

A zone is an area that has a particular characteristic, purpose, use and/or set of specific restrictions. By using zones, you have an effective strategy for reducing many types of risks. While securing your environment in a more granular and effective manner, you will lower the costs associated with it. Instead of protecting everything with the same level of protection, you now can associate systems and information to specific zones. In addition, systems that are subject to regulatory compliance can be grouped in subzones to limit the scope of compliance checking, which reduces the cost and time needed to complete lengthy audit processes.

Tip #10: Segregation of duties

Segregation of duties is a basic building block of sustainable risk management and internal control for a business. The idea behind this is to spread the tasks and privileges for security tasks among multiple people. No one person should be able to control everything, which means that no one person has the ability to delete everything either. For example, one person should control the production environment, another person should control the backup environment. Even within backup practices, having a secondary and offsite (i.e., DR) copy of your data that is under different credentials and management control than the primary backup system is often considered a best practice.

Tip #11: Digital hygiene

In our day-to-day life, we take personal hygiene and cleanliness seriously. We all know that washing our hands helps prevent the spread of infectious disease and keeping clean is a fundamental part of our daily routine.

With the increase of threats, vulnerabilities and expanding digital contacts, you always are at risk to catch the digital flu. Just like with the real flu, there are ways to decrease risk while moving through the digital world by following some elemental digital hygiene practices. Following a good digital hygiene practice can keep your data healthy, your privacy protected and your security intact.

Important practices:

- Create unique passwords for each login source. This way, you can ensure that if one password gets breached, your stolen password won't give hackers access to your other accounts
- Use a password manager. It's hard to remember over 100 passwords. A good password manager can help you manage all your login information, making it easy to create and then use unique passwords
- Use multi-factor authentication (MFA). You can configure MFA to ensure additional account security.
- Use a robust password policy
- Use an account lockout policy
- Remove unused devices, applications, departed employees and non-essential programs and utilities
- Patch management: make sure that all in-use software, hardware and firmware are running up-to-date software levels

Tip #12: Backups

Digital hygiene is a key ingredient for resilience. If you're doing regular backups, cyberthreats become more of an inconvenience than a disaster. You may lose a day of work, but you won't lose everything. How often you back up specific data types and whether you use a cloud service, or a physical device is one of the choices you need to make based on required service and security levels.

Ransomware will lock you out of your own data by encrypting your files. As such, proper backups are an excellent way to recover from this kind of attack. With backups, it becomes easy to replace your encrypted files with copies you have in your recent backup repository. You may lose some of the most recent data when you revert to backups, but it certainly beats paying a cybercriminal to restore the files for you, assuming they honor their agreement to do so.

Tip #13: Encryption

Use encryption to make sure that only authorized parties can access your information. As soon as your information leaves a defined security domain, make sure that your information is encrypted to an appropriate pre-defined level. Encryption itself does not prevent interference, but it does prohibit unauthorized parties from reading your information. Encryption helps protect sensitive data if other security measures fail.

Veeam opportunities for protection

It should be expected that a data protection product would excel in the protect function of the framework, and Veeam fulfills this expectation. Veeam provides backup solutions across a wide spectrum of virtual, physical, file, Software as a Service (SaaS), container and cloud platforms. By focusing on **Veeam Backup & Replication**, the capabilities listed below align to the protection function of the framework.

If you learn one thing from this paper, know that you need to have backup data on a form of ultra-resilient storage media. Ultra-resilient backup storage means that you have one or more copies of backup data on the following media:

- Immutable backups in AWS Amazon S3 and S3-Compatable storage systems
- Immutable backups in Linux with the hardened repository
- Tape media removed from library or marked as WORM (Write Once Read Many)
- Veeam Cloud Connect with insider protection
- Offline (i.e., ejected) removable media or rotating drives

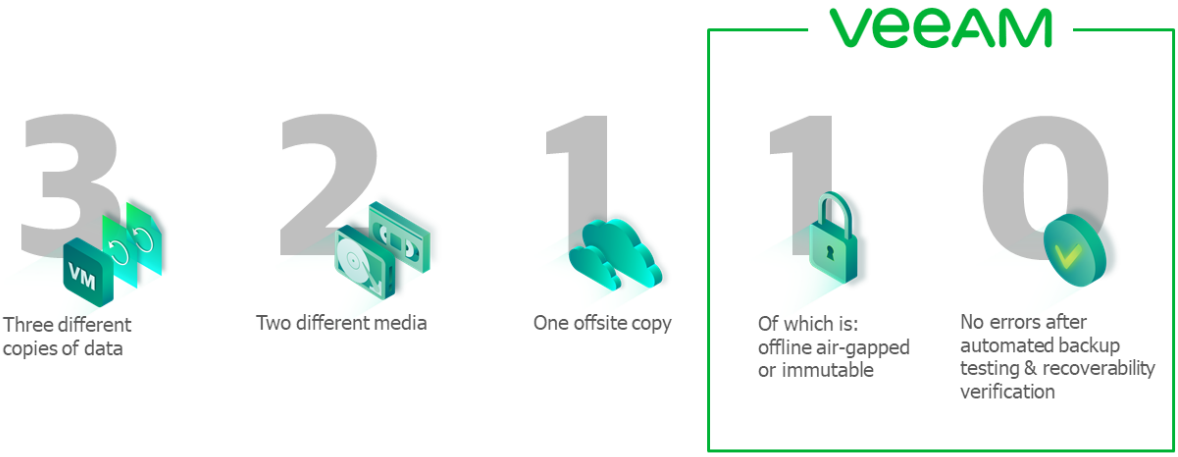
Backups in ultra-resilient storage are one of the most critical mechanisms for achieving ransomware resiliency. Organizations should select which approach (i.e., media, storage type, etc.) makes the most sense for the specific data type and business process. Beyond ransomware, these options can bring other protection techniques for backup data resiliency, like mitigating insider threats and preventing accidental deletion or corruption.

The 3-2-1-1-0 Rule

For many years, Veeam has advocated for using the 3-2-1 Rule as a general data management strategy. The 3-2-1 Rule recommends that there should be at least three copies of important data, on at least two different types of media, with at least one of these copies being off site. The wonderful part about the 3-2-1 Rule is that it does not require any particular type of hardware and is versatile enough to address nearly any failure scenario.

However, as the threat of ransomware has advanced, Veeam has emphasized that the "one" copy of data be ultra-resilient (i.e., air-gapped, offline or immutable). This recommendation is imperative to becoming resilient against ransomware.

This is reflected in the 3-2-1-1-0 Rule, which addresses this ultra-resilient copy requirement. The 3-2-1 Rule has advanced to recommend that one copy of your data be immutable, offline or air-gapped, which means zero backup errors with Veeam's industry-leading SureBackup® automated recovery verification.



Recommended reading:

These techniques represent the most modern immutable capabilities in Veeam's portfolio.

You can read more about the hardened repository at vee.am/hlrpaper

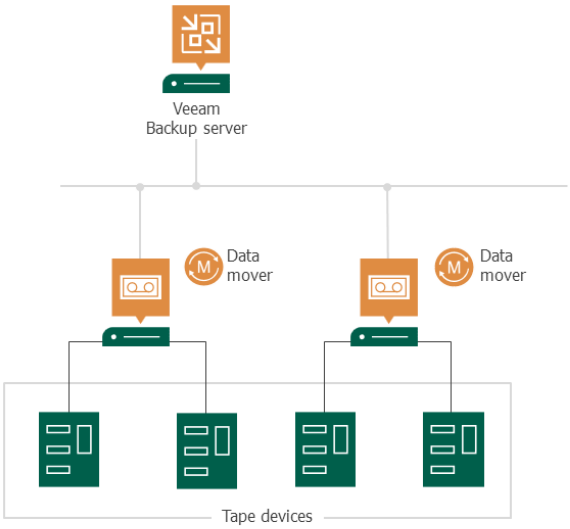
You can read more about the immutable backup capabilities for S3 and S3-compatible storage systems with Veeam at vee.am/ImmutableCapacityTier

Each of the ultra-resilient media types are explained below.

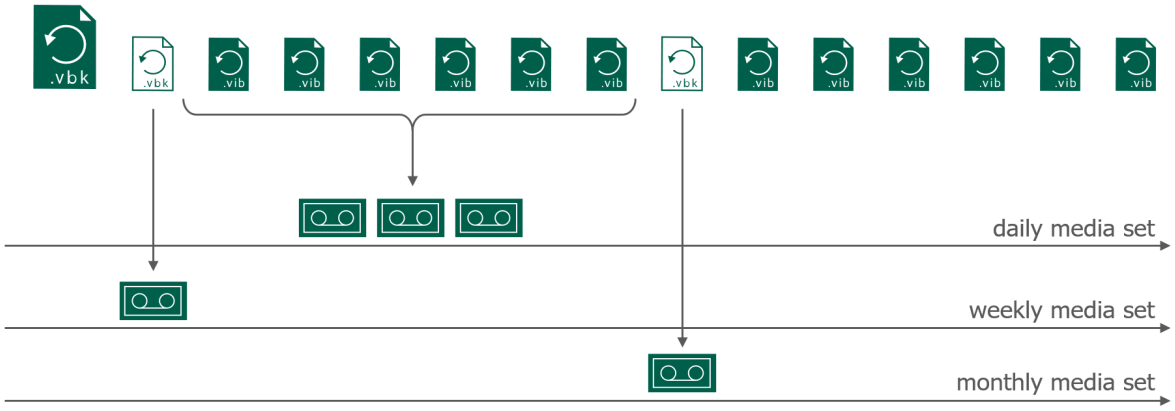
Backups on tape

Every IT organization has their opinion on tape media, but the acquisition cost, offline capability and portability of tape is hard to beat. Tape media that's ejected or exists out of a library is automatically offline.

Veeam supports write-once read-many (WORM) media for additional resiliency against ransomware, and has broad and tape-native media support, including writing files and full backups to tape. Veeam tape support for VM and physical server backups are visualized in the model below:



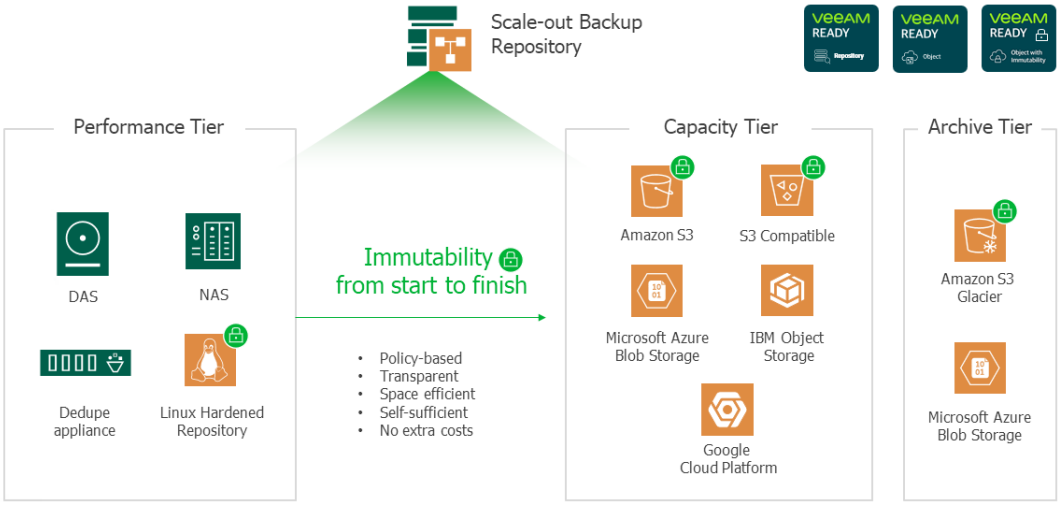
Tape support in Veeam is flexible. It supports configurations of modern LTO tape devices (i.e., LTO 3 and above) and libraries, and there are several ways that tape can be used to bolster ransomware resiliency. One way is to only put a fixed amount of data over a shorter amount of time on tape media, like a few weeks' worth of backup data. When people think of tape infrastructure, they often think of massive media libraries with years and years of data. However, you can leverage tape as an ultra-resilient storage media type for relatively nearline operational recovery restore points. Media sets in Veeam are visualized in the figure below, which shows a sample daily, weekly and monthly media set.



One oversight when it comes to organizations who are combatting ransomware is that tapes are not always removed from the library. If the threat actor that's operating the ransomware takes over control planes on the network, erasing backup storage can be an attack vector. Also consider the use of WORM media with media removed from the library. This is an extremely resilient example, since the copy of data is offline, air-gapped and immutable in this form. Veeam can also be configured to automatically run a tape backup operation as soon as another backup activity completes, like primary backup to the disk-based hardened repository.

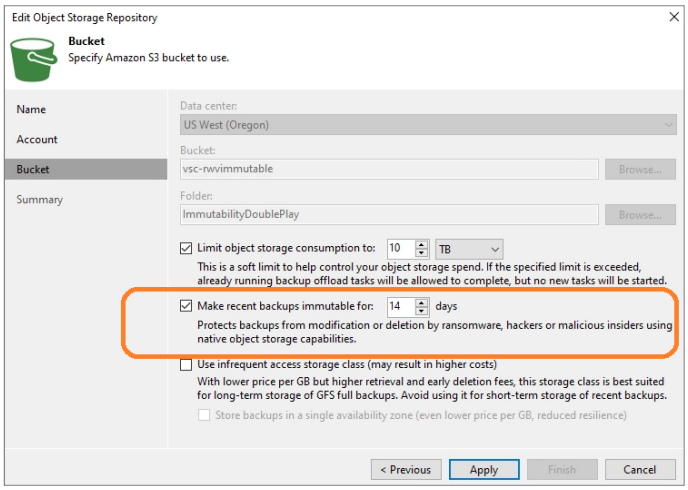
Immutable backups in S3 or S3-compatible object storage

Veeam Capacity Tier supports immutable backups as a powerful technique to become resilient against ransomware and other threats. This is achieved with the Veeam Scale-out Backup Repository™ (SOBR) with Capacity Tier (formally known as Cloud Tier) enabled. Capacity Tier is a policy-based capability that writes backup data into object storage. AWS and AWS S3-compatible Microsoft Azure, Google Cloud and IBM Cloud object storage targets are supported, but only the public AWS S3 and select S3-compatiable storage systems support object lock with the compliance mode needed for Veeam backup data to be placed in a bucket as an immutable backup. See this link for an [updated list of supported solutions.]



The wonderful aspect about S3-immutable backups is that they could not be easier to configure within Veeam Backup & Replication. There are two properties that should be configured for the most resilient usage of Veeam Capacity Tier. The first is AWS S3 or S3-compatible buckets, which should select the option to make backups

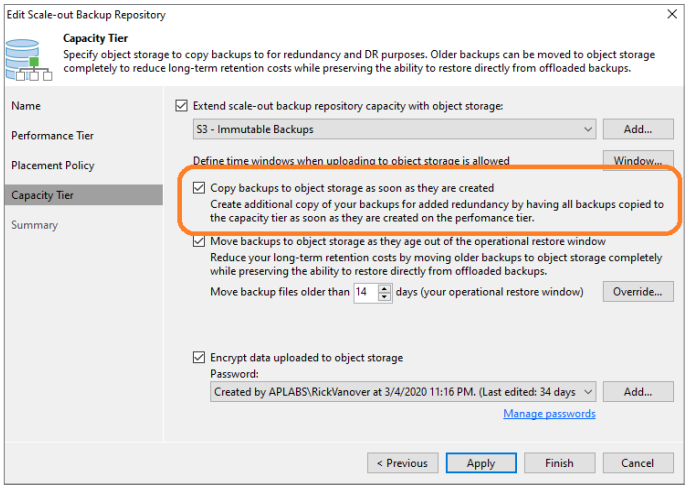
immutable for a specified number of days. This applies to all backup data that's going into the bucket from the SOBR tiering process that happens either after a backup is completed (a.k.a. copy mode) or after a specific time interval (a.k.a. move mode). The process of setting the immutability period on a bucket is shown below:



The immutability setting is a property of the object storage bucket. To effectively use object storage and be resilient against ransomware, an additional setting should be used as a property of SOBR in the upload settings. Capacity Tier object storage will then ingest backup data by moving backup data to object storage for backup files that are older than a specified operational restore window (i.e., 14 days or older). There is also an option to copy backups to object storage as soon as they are created (a.k.a. copy mode).

Copy mode is another important step in becoming resilient against ransomware, since it will immediately make a copy of the backup data in object storage after a backup operation on the performance tier is completed. As backups age, move mode will still remove or tier the backup data from on-premises extents from the performance tier. In the time between backup creation and the operational restore window, backups will exist both on-premises and in object storage. Couple that with immutable settings, and there is a strong ransomware resiliency technique in place, which fully supports the 3-2-1-1-0 best practice.

This is important because, in many cases, restores from the most recent points are the most desirable because they have the nearest recovery point objective (RPO). The process of configuring copy mode for SOBR is shown in the figure below:

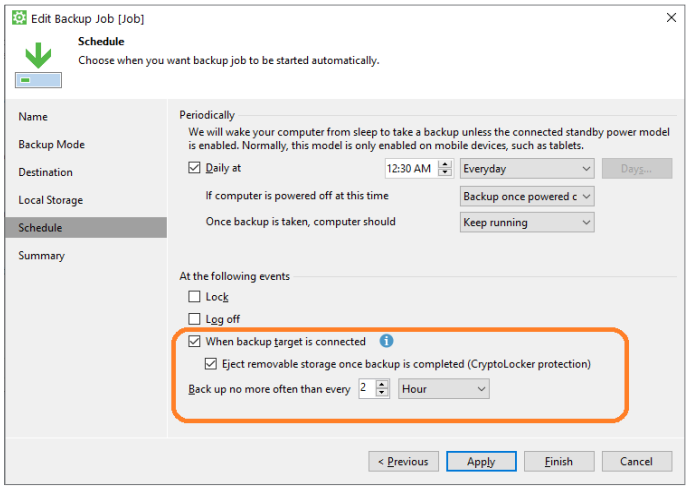


The option to encrypt backup data in object storage is also shown in the figure above. It goes without saying that this is a recommended configuration for backup data in the cloud.

Air-gapped and offline media

Rotating drives and removable drives are other media types that have offline characteristics similar to tape. For larger data volumes, this becomes more difficult to manage since single drives that can come offline are generally limited by drive sizes (although these sizes are increasing). This approach can be adopted situationally as well, for endpoints and edge locations like ROBO. Veeam Backup & Replication supports repositories that rotate media for interchanging processes, like offsite storage.

Veeam Agent for *Microsoft Windows*, for example, supports removable media targets. For endpoints, this solution has the additional capability to eject media upon the completion of a backup job, making the removable media offline. This option is shown in the figure below:

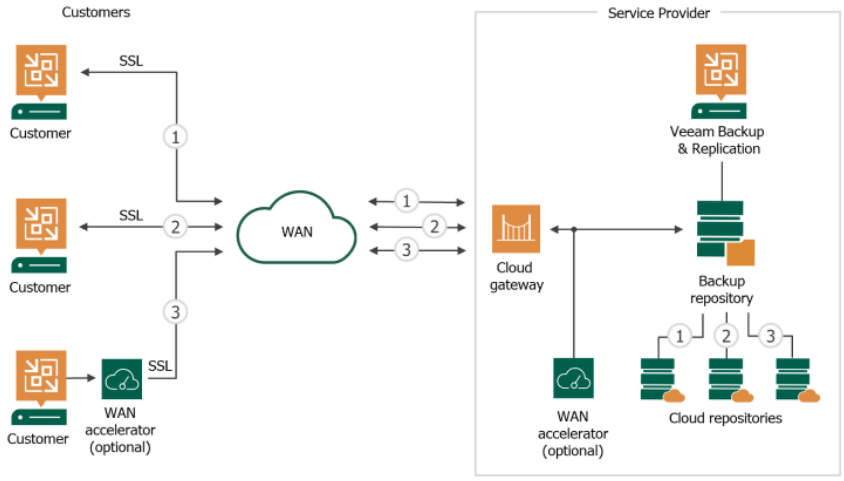


Aside from ejecting the removable storage once the backup is completed, organizations should know that doing this does not guarantee bulletproof protection against ransomware. To ensure that your backups are safe, keep your OS up to date and regularly scan your backup repository for virus threats with modern antivirus software, including using the latest virus definitions.

Backups in Veeam Cloud Connect with insider protection

Veeam Cloud Connect, a capability of Veeam Backup & Replication, is a long-established technology that provides Veeam Backup Storage as a Service as well as Disaster Recovery as a Service (DRaaS) that's powered by Veeam replication. Veeam Cloud Connect is enabled by Veeam-powered service providers. This technology can be packaged as "Veeam Cloud Connect for the Enterprise" so that larger organizations can offer this capability in-house.

Veeam Cloud Connect Insider Protection was created to provide additional resiliency for backup data from the risk of ransomware, malicious administrator activity or accidental deletion. With insider protection, an additional out-of-band copy of the backup data will be retained by the service provider and exposed by interventions like a support call. This process will allow backup data to be re-populated into the Veeam Cloud Connect repository, and then drive restores on-premises. Veeam Cloud Connect Backup is represented below:

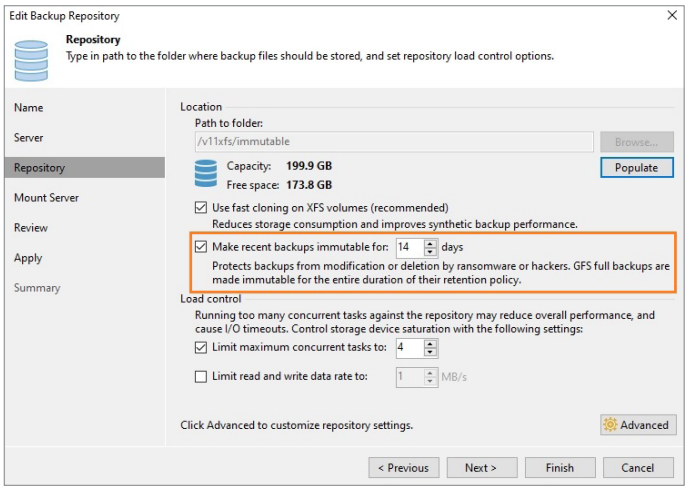


You can find a service provider that offers Veeam Cloud Connect with Insider Protection here.

Immutable backups in a hardened repository

Veeam Backup & Replication provides the ability to store backups in a Linux Hardened Repository, which uses a Linux system to write backups to a file system with immutable attributes. This is used in conjunction with a single-use credential, which enhances the security of backup data. This is an important way of writing data in an immutable fashion, and it serves as a strong step in the **protect** function of the framework. It also gives high confidence of recovery for the **respond** function.

The hardened repository is Linux-based. It's important to emphasize that the Linux operating system of the hardened repository needs to be protected from unwanted or malicious access (physically and via network access). It is recommended that you isolate this server as much as possible to protect the integrity of the backups in it. The Linux Hardened Repository is shown below with 14 days of immutability configured:



Encryption

The threat landscape is constantly evolving and moving, and we see double or even triple extortions becoming more and more popular. The first extortion is about getting your own encrypted data back from a ransomware

attack. The second is about data that's exfiltrated from your environment, which you must pay to get back and/or prevent it being published or auctioned off. The third extortion is where stolen data, through exfiltration, contains customer information. So, your customers are being approached and extorted to pay a ransom to circumvent that information from being published or auctioned off. It's becoming increasingly important to consider encrypting backup files because of the increasing threat of data exfiltration from stolen backup files, which often contain a full copy of your digital environment.

The encryption technology in Veeam Backup & Replication allows the product to protect data both while it is in transfer between backup components and when it's at rest, stored at its final destination (i.e., backup repository, tape, cloud repository or object storage). 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.

Importance of protection in the framework

The ability to protect data is critical, since it will predicate the experience of the other functions of the framework. Veeam's recommendation to have at least one copy in an ultra-resilient form is paramount in this step.

Some organizations are pursuing double-play or triple-play immutability options, like using the SOBR with the hardened repository on-premises and using immutability in the Capacity Tier with S3 Object Lock. The triple-play option would be the double-play configuration with an additional copy residing on tape WORM media.

Detect

The detect function allows for the timely discovery of cybersecurity events. The detect function is a critical step to a robust cyber program; the faster a cyber event is detected, the faster the repercussions can be mitigated.

"The question you should ask yourself is: which mechanisms are appropriate to implement to ensure swift identification and detection of cybersecurity incidents?"

Cybersecurity best practices for detection

To know when you're under attack or breached, it is vital to have visibility into the end-to-end data flow of your information. You should be able to know what is normal behavior and what is not. Make sure you monitor your accounts and infrastructure for suspicious activity. Best practices for detection are:

Tip #14: Detection systems

There are several systems that can alert you about suspicious behavior so that you become aware of someone snooping around and trying to gain access to your infrastructure. It is important to get alerts as soon as possible when defending against other attacks like viruses, malware and ransomware. The biggest risk of these attacks is that they may propagate to other systems quickly. So, having visibility into potential ransomware activity is key.

Tip #15: Tripwires

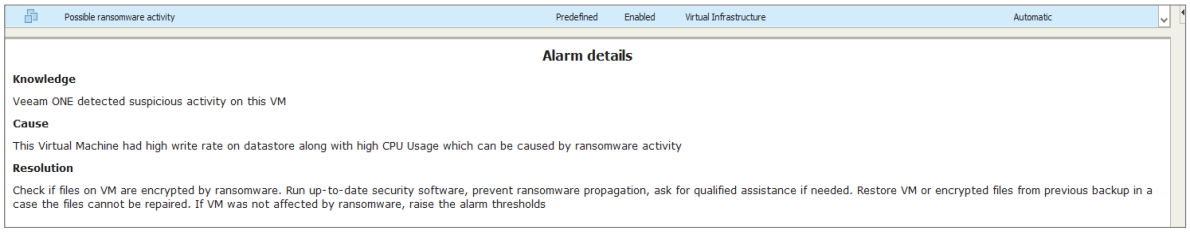
Place virtual tripwires, like an unused admin account with alarms tied to it. When any activity on that account is observed, it will trigger a red alert instantly.

Veeam opportunities for ransomware detection

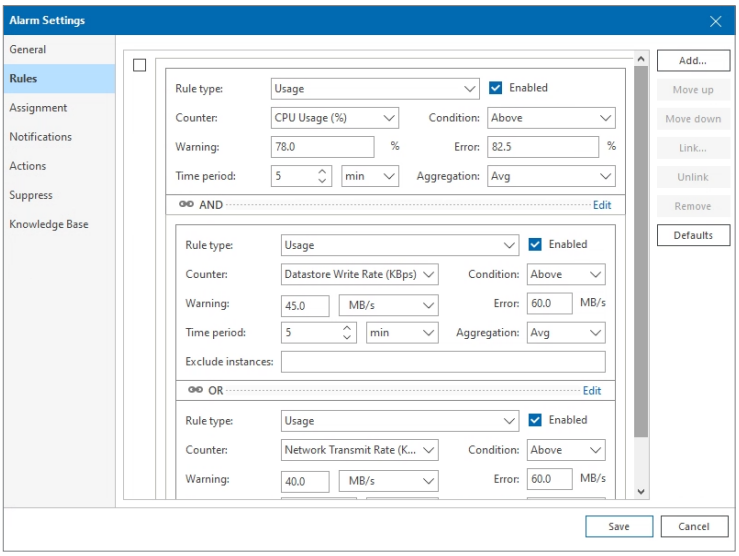
Detecting a ransomware threat as early as possible gives IT organizations a compelling advantage, and the potential of this cannot be underestimated. Veeam has implemented two specific detection techniques to help detect possible ransomware activity:

Possible ransomware activity alarm

This Veeam ONE™ alarm detects a combination of high CPU activity and sustained write I/O to a drive or high network transmit rate. This alarm is shown in the figure below:



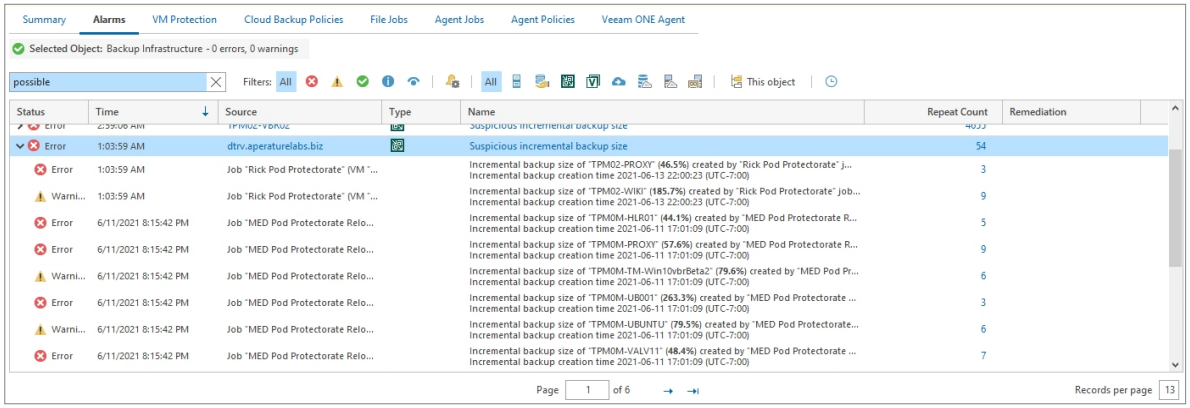
This alarm is customizable. The defaults are a good starting point for possible ransomware activity, but they can be adjusted to be more conservative in regard to what triggers this particular alarm. This customization is shown in the figure below:



With Veeam ONE, this next piece of advice is critical in addressing what happens when this alarm is triggered. Veeam recommends several actions that are built into the alarm to provide more aggressive notifications to IT staff. This includes SMS messaging, alerting security teams and potentially extreme steps like powering off a VM or disconnecting the network interface via the actions in the Veeam ONE alarm. If you have both VMware and Hyper-V systems in place, make sure these actions are required for both environments.

Suspicious increment size

This alarm applies to Veeam ONE when it is monitoring Veeam Backup & Replication in the data protection view. This alarm will report that an incremental backup is suspiciously large. This logic is based on the normal change rate, and the possibility that the source data is encrypted, which would remove most storage efficiency opportunities. Like most Veeam ONE alarms, there are configurable rules to select how deep the analysis is performed. By default, it will analyze three restore points and indicate a warning at a 150% change rate, and an error alarm at a 200% change rate. This alarm is shown below:

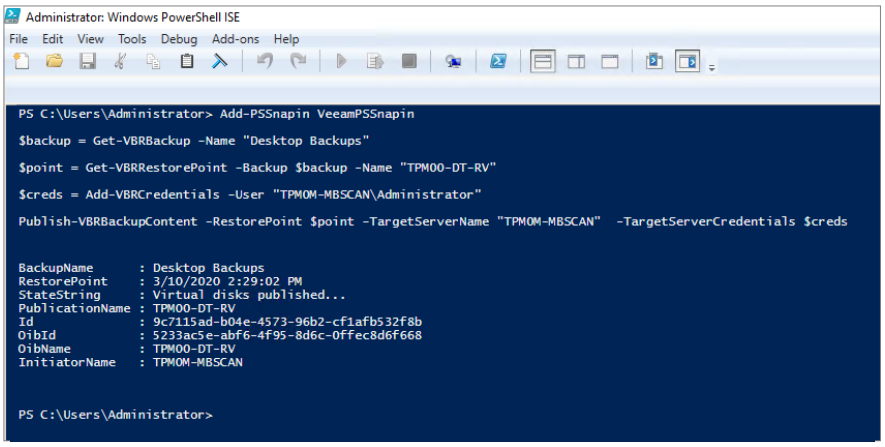


Data integration API

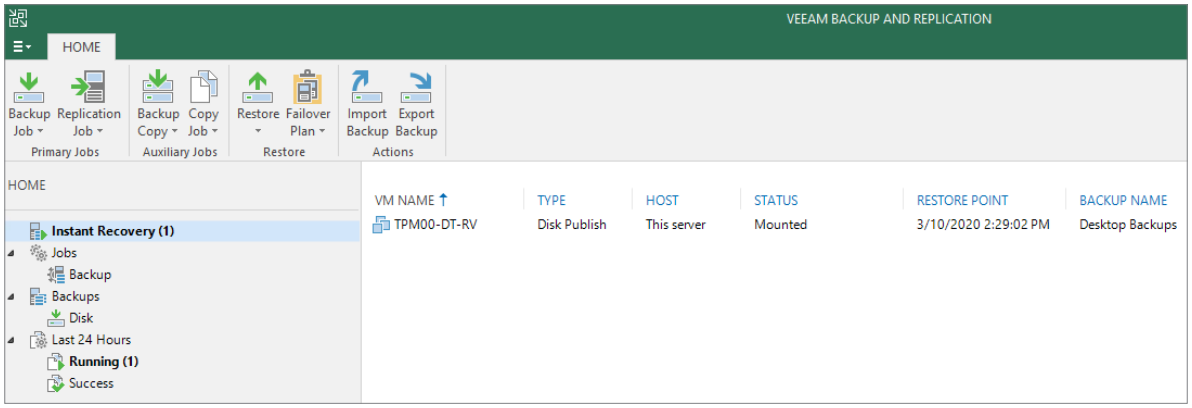
The Veeam data integration API is best consumed through PowerShell and is part of Veeam Backup & Replication v10 and later releases. This capability allows the data of backup files to be exposed as a mounted folder, and it allows access to data that is available in backups created by Veeam Backup & Replication. This capability is an excellent new technique that can be used as a weapon in the war against ransomware, and additional scans can be done on data that has already been backed up.

This ransomware resiliency technique can provide additional scans of backups for threats, including using additional, more-invasive tools that may not be used on production workloads. Additionally, if endpoint backups are in Veeam repositories, there is an incredible surface area to analyze for potential threat introduction.

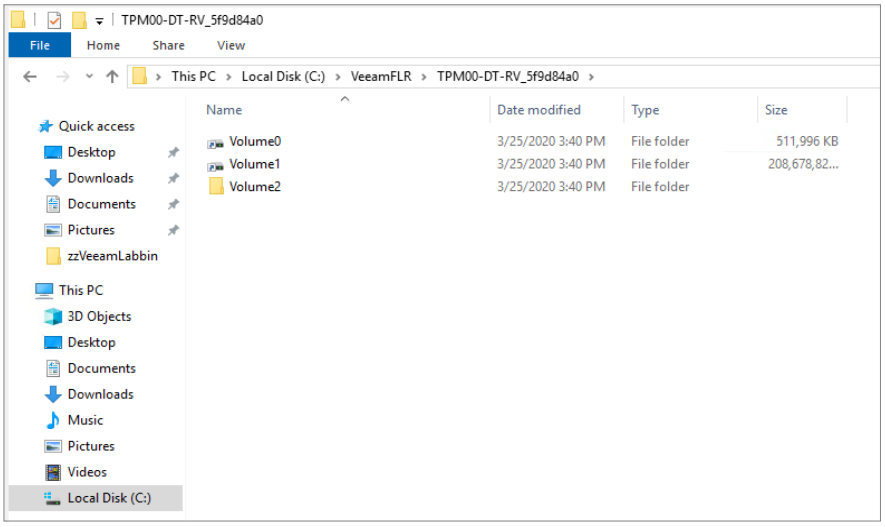
Using the data integration API will start with backups in a Veeam repository. The example PowerShell script will call the backup of a system (TPM00-DT-RV) to be mounted via the Publish-VBRBackupContent cmdlet. This is shown in the figure below:



This is a sample PowerShell script for one backup being mounted, however multiple backups can be mounted with the cmdlet. This script will perform an instant disk publish task in Veeam Backup & Replication. This action is similar to an Instant VM Recovery®, which Veeam pioneered over a decade ago, but instead of publishing the storage of the backup VM or agent to a VMware or Hyper-V environment, it publishes to the Veeam Backup & Replication server (or another dedicated system with the role to do the scans). This publishing is done transparently through iSCSI from the cmdlet (and through FUSE for Linux in V11). This Veeam Backup & Replication server shows the backup exposed as disk publish below:

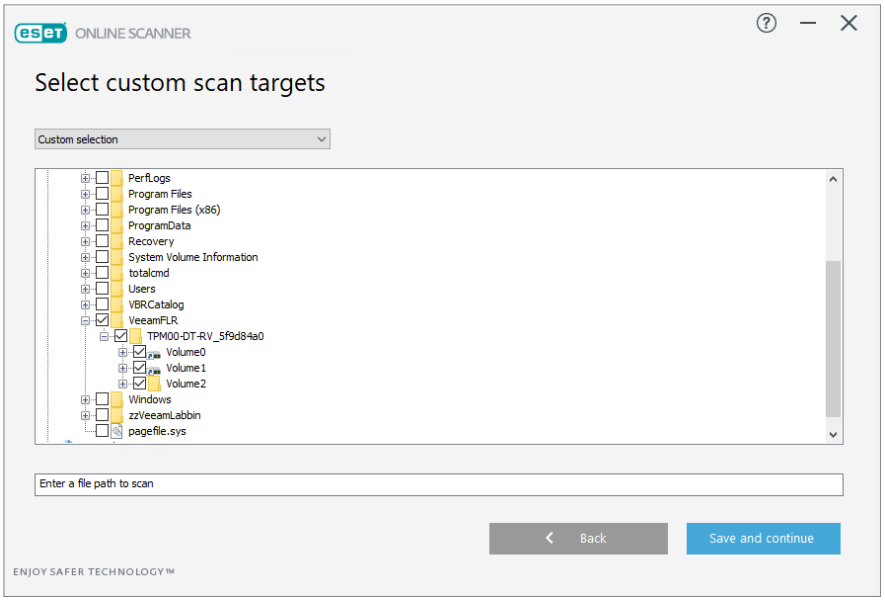


This is a sample PowerShell script for one backup being mounted, however multiple backups can be mounted with the cmdlet. This script will perform an instant disk publish task in Veeam Backup & Replication. This action is similar to an Instant VM Recovery®, which Veeam pioneered over a decade ago, but instead of publishing the storage of the backup VM or agent to a VMware or Hyper-V environment, it publishes to the Veeam Backup & Replication server (or another dedicated system with the role to do the scans). This publishing is done transparently through iSCSI from the cmdlet (and through FUSE for Linux in V11). This Veeam Backup & Replication server shows the backup exposed as disk publish below:

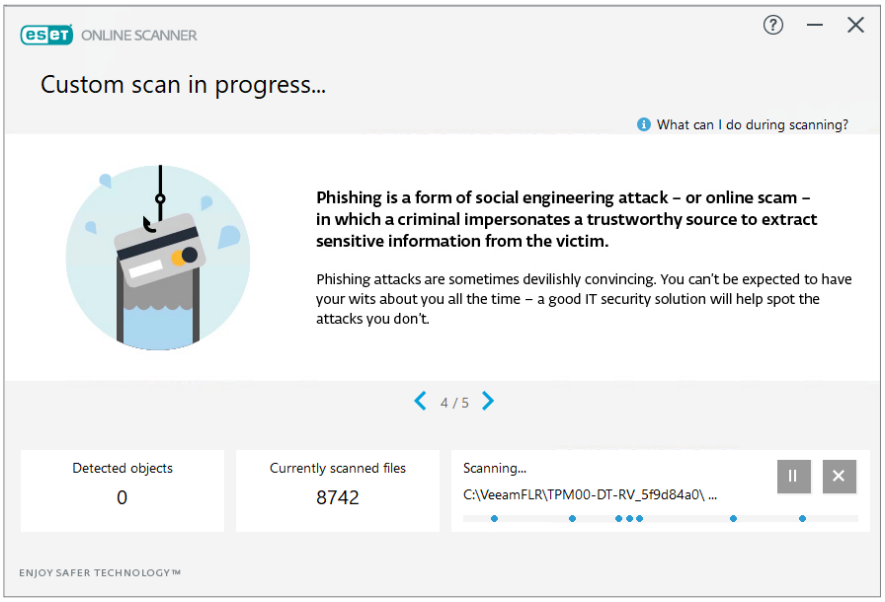


This is the point where you can unleash the power of your backup infrastructure. The systems that are backed up with Veeam can then have advanced scanning performed on them. Two specific examples that can aid in detection are ESET scanning tools and Total Commander. In both scenarios, this can be done with no exclusions and from within the backup copy operation. Many other tools can be used for this process, which is unique since it can be used with more aggressive scanning and the latest definitions.

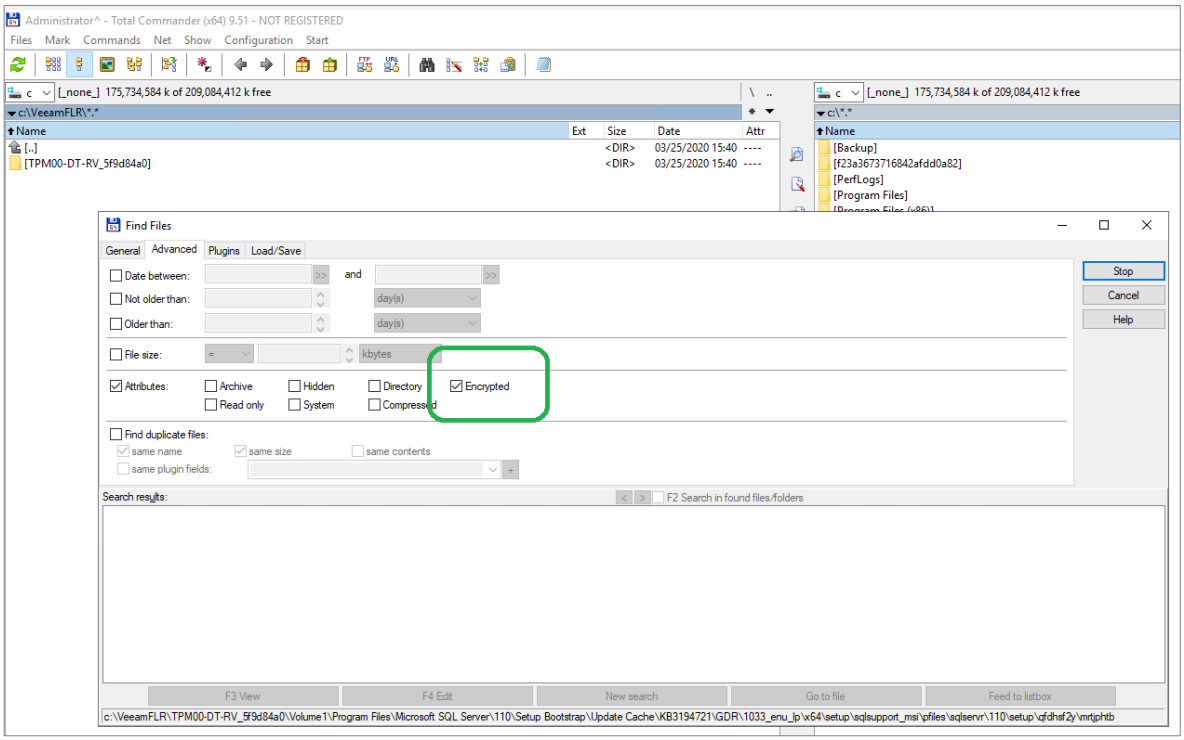
In the first example, ESET can be used to scan just the VeeamFLR (file-level recovery) path that contains the published backups.



Once the VeeamFLR path is selected in the ESET tool, a custom scan can be performed. The ESET tool will then download the latest threat definition file before the scan to have the most up-to-date information to scan against. The scan progress is shown below:



Another tool you can use as a possible detection technique when using the data integration API is Total Commander. This tool is a staple that many IT administrators use for advanced storage functions. One of the interesting capabilities of Total Commander is that the search can look through the VeeamFLR path for files that are encrypted, as shown below:



Due to the inherent fragmentation of ransomware threats, it is possible that the encryption search may not show files that are encrypted from a threat. The capability of Veeam Data Integration API in coordination with some of the preferred toolkits in each IT organization's area of expertise is compelling in bolstering the visibility of threats before they are exposed at a larger scale. There is also incredible opportunity to use the Veeam Data Integration API in larger automation scenarios. Consider implementing workflows that take backups, perform SureBackup-automated backup verification jobs, and then automatically use the Data Integration API to perform more intensive scan tasks, post-backup, that may not be done on production workloads. This is an opportunity to reduce the time from threat introduction to threat exploit.

Go deeper with the Veeam Data Integration API

You can find more information about the Veeam Data Integration API and associated cmdlets here

Veeam DataLabs

Veeam DataLabs™, a set of powerful features within Veeam Backup & Replication, can be used to help you become resilient against ransomware by serving as both a detection and remediation method. The SureBackup job will run Veeam DataLabs to perform many tasks, including:

- Ensuring recoverability of a backed-up system
- Performing a test on system-like updates, changes to an application, etc.
- Veeam DataLabs Staged Restore and Veeam DataLabs Secure Restore technologies

From a ransomware detection standpoint, if a threat is exposed on the next boot of a system, a SureBackup job could identify an issue that means a system will not boot, or that applications 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 in remediating ransomware threats.

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

Respond

The respond function helps users develop techniques to contain the impact of cybersecurity events by making sure that you develop and implement the appropriate actions to take in a detected cybersecurity incident.

"The question you should ask yourself is: how can I mitigate a cybersecurity event and make sure the impact is contained as soon as possible?"

Cybersecurity best practices for responding

The faster and more effectively you respond to a possible detection of a cyber incident, the faster you can stop the threat in its tracks or mitigate its damage and reduce any potential financial impact. Widely used best practices for the respond function are:

Tip #16: Create an incident response plan

One of the obvious ways you can prepare for cyber security incidents is to create an incident response plan. Creating a clearly defined incident response plan will enable you to outline procedures for detecting, communicating, controlling and remediating security incidents so that employees know how to best respond to cybersecurity events when they arise.

Tip #17: Stay calm

A ransomware attack is extremely intrusive to any organization, especially for the people that work in that organization. Blaming the IT employees, or any person in your workforce, will not help you respond well to the cyber incident at hand, and could even make things worse! Expect people to react differently than they would normally. Knowing that someone has been in your infrastructure or data, and the uncertainty surrounding what and how it happened, will likely create fear and generate higher levels of stress. This can make your workforce afraid of their own infrastructure. Stay calm and get the right people together to activate the incident response plan as quickly as possible.

Ransomware response advice

Ransomware response is a course of action that often leads to recovery scenarios. In fact, at Veeam, our mindset is that if ransomware is on a system or a file data source, the only course of action is to recover that data. Having the response function ready for action will ensure success in the recovery function. The reality is that any response will depend on the nature of the incident, but one thing will remain consistent across all recommendations: now is the time to prepare a robust response plan.

In fact, this step is explicitly recommended by the Cybersecurity & Infrastructure Security Agency (CISA) guidance for ransomware. If you haven't yet, it is highly recommended that you review the resources at the CISA ransomware site.

Also note this ransomware guide.

This document highlights a number of critical recommendations, but one thing that we have seen is that organizations do not have a complete response plan to handle a ransomware incident.

The CISA ransomware guide specifically recommends that you:

"Create, maintain and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident."

This is a very important point, and we want to draw your attention to the Veeam Disaster Recovery Orchestrator solution. This product is specifically designed to automate and document DR and cyber resiliency response via restore, failover, storage and Continuous Data Protection (CDP) protection plans.

Veeam opportunities for ransomware response

The response phase is a critical function in the process, and Veeam has many capabilities that align to a successful outcome. The response function is enabled by Veeam Disaster Recovery Orchestrator, which automatically validates service level agreements (SLAs) for recoveries to go as planned and creates dynamic documentation and reporting on the environment with Veeam ONE.

Automatic DR plans with Veeam Disaster Recovery Orchestrator

Veeam Disaster Recovery Orchestrator is a powerful add-on to Veeam Backup & Replication. It provides critical capabilities for response functions needed to recover from disasters of many types, including ransomware. There are four types of plans available that can provide organizations with a clear path to optimal response, including the kind of expectations you should have for a response and recovery function. These four plan types are based on Veeam replicas, backups, supported Storage Snapshots and Veeam Continuous Data Protection (CDP) replicas.

As part of a plan creation, a DR plan document is automatically generated, along with a full audit log of changes as they occur. This saves time and reduces the risk of human error and/or issues with configuration drift. The figure below shows a DataLabs Test report that indicates that the target Recovery Point Objective (RPO) and the Recovery Time Objective (RTO) are both met:

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

DR tests in Orchestrator can be scheduled to run daily or on-demand. The testing environment can be left running after a test to provide access to a copy of production data, which can be leveraged for patch and application testing and security scanning to further enhance information security efforts.

Plans in Orchestrator will also be automatically checked to ensure that the environment is ready for failover at any moment, which allows organizations to confidently recover when needed.

Testing DR plans is key to ensuring that they can be used successfully to recover from ransomware. Automated verification and reporting can also be a component of internal and external compliance initiatives.

Additional Veeam response considerations

Beyond orchestrated recoveries with Orchestrator, there are several response considerations to raise:

Communications first: In disasters of any type, appropriate communication becomes one of the first challenges to achieve. Have a plan for how to communicate to the right individuals out-of-band. This would include group text lists, phone numbers or other mechanisms that are commonly used for on-call activities but expanded to entire IT operational groups. When speaking to organizations who drive a successful ransomware response and recovery scenarios, they consistently mention how critical effective communication is. Related to this can also be chain of command and decision-making hierarchies. One of the hardest parts of recovering from a disaster is decision authority. Who makes the call to restore, failover, etc.? Make business discussions about this before an incident arises.

Force password resets: Users don't like this, but management should implement a sweeping forced change of passwords on a regular basis. This will reduce the threat propagation surface area.

Veeam support: There is an elite group within the global Veeam support organization that has specific procedures to guide customers through data restoration in ransomware incidents. If needed, use this team, since you don't want to put your backups at risk. This team is critical to your ability to successfully recover.

Experts: Have a list of security, incident response and identity management experts that are ready to be contacted when needed. They can be within your organization or external experts. If a Veeam service provider is used, there are additional value added onto their base offering that can be considered (such as Veeam Cloud Connect Insider Protection). Options in this area can also be sought from cyber insurance organizations.

Recover

The recover function supports timely recovery to normal operations to reduce the impact of a cybersecurity event. This function makes sure that you develop and implement the appropriate activities to maintain plans for resilience and restore any impaired capabilities or services due to a cybersecurity event.

"The question you should ask yourself is: what activities do I need to deploy to increase my digital resilience and have restore capabilities in place that can restore impaired service due to cybersecurity events in a timely fashion?"

Cyber security best practices for recovering

As the number of cyberattacks and data breaches continue to rise, your organization will inevitably experience a security incident at some point. There are three kinds of organizations in the world — those who have been hacked, those that are next in line or, worst of all, those that don't know they've already been hacked. The only thing you can, and should, do is buy as much time as possible by deploying the right countermeasures in people, processes and technology. Unfortunately, not all attacks can be averted, so make sure that you have a recovery strategy in place for those moments when your cyber security defences have been breached. Best practices for recovering are:

Tip #18: Recovery strategy

Have a recovery strategy in place. Before you realize your infrastructure is breached, you should know what to do when you're compromised through an attack. Defining a prioritized list of action points that can be used to undertake recovery activity is critical for timely recovery and containing the damage of an event. Back up your data, and make sure the backups cannot be accessed by an attacker. An offsite copy (a.k.a. air-gapped) or read-only (a.k.a. immutable) copy of data on any media is highly recommended to survive any attack. Remember the 3-2-1 Rule!

Tip #19: Design for recovery

There is only one reason we perform backup, and that is to recover. This means that backup systems must be designed with recovery performance in mind, rather than simply focusing on the amount of time the backup will take. In environments with SLAs, the design of a backup environment should start with determining what the recovery SLAs are. When the right RPO and RTO values are known, work backwards, keeping the laws of physics in mind to design a backup system that can achieve these business requirements. This way, the backup system is designed to deliver the required performance, rather than assuming that the backup system will be able to meet recovery requirements. Sadly, too many organizations incorrectly believe that they are far more recoverable than they actually are.

Veeam opportunities for ransomware recovery

Veeam Backup & Replication backups provide a set of versatile recovery options, like one would expect from a leading provider of data protection solutions. This versatility starts with the portable data format of the backup files that can be restored to new locations if needed. This is important in a scenario where the source platform (a.k.a. data center) can't be trusted to restore to.

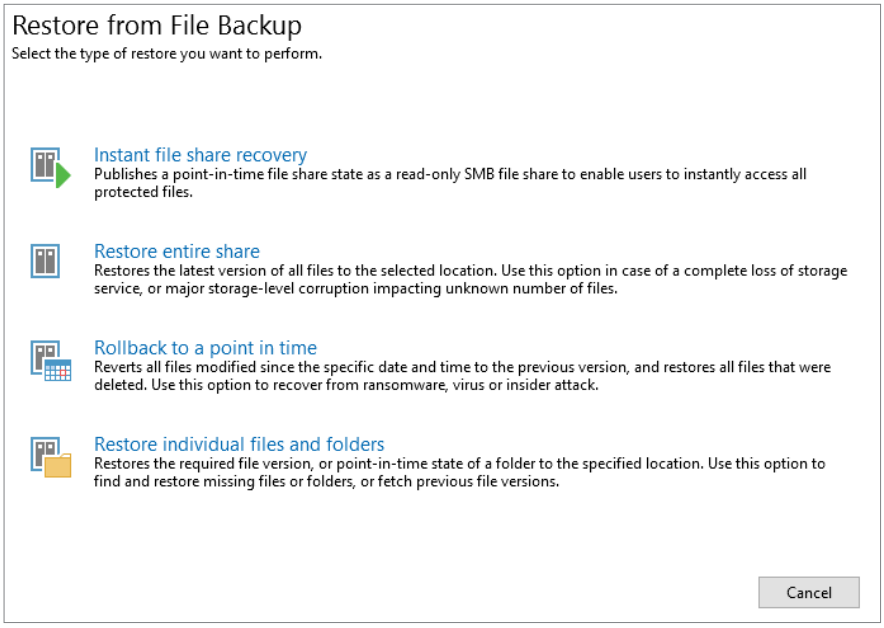
Image-based backups with Veeam can be restored to a service provider, to a hypervisor (VMware vSphere, Microsoft Hyper-V Server, Nutanix AHV and Windows 10 Hyper-V) or to the public cloud as alternate restore locations if needed.

NAS recovery options

One of the popular targets for ransomware are NAS devices, due to how they store large amounts of critical data. Coupled with insider threats, device failures or accidental deletion, there are many reasons why file data needs to be considered a threat target as well. Veeam Backup & Replication's support for NAS backups will provide good recovery options for file share data if a ransomware incident has compromised the contents of that file share.

The Veeam file backup engine has four types of recovery. The first type is file and folder recovery for isolated situations that recover based on the last time the backup was run. The second recovery type is to revert the entire share to a specified restore point. The third recovery scenario is to restore the entire share to a new device for a loss-of-device scenario. The fourth type, instant file share recovery, is an excellent way to quickly publish the contents of the share for the fastest access to data.

Each scenario has a ransomware use case for recovery, but the second scenario provides a compelling way to recover a share if a ransomware incident has occurred. If the threat is removed, but part of the NAS share has been encrypted or deleted, this restore type can take the contents of the share back to what it was at prior to infection. For NAS systems that have millions of files and very deep folder paths, the Veeam cache repository for the share will keep track of the file and folder changes within the share. This allows you to restore to the point-in-time without having to know the damage to the contents of the share. The NAS restore options are shown below:



Additional Veeam recovery considerations

It is hard to forecast exactly how a disaster will proceed but having many options to deal with a threat is a sound approach. One of the versatilities of Veeam backups is the absolute portability of the backup data. This means that backups can be restored to completely new targets, the cloud, other hypervisors or bare metal. Below are some additional considerations for recovery:

Ready to restore: when the conditions are right to restore, implement additional safety checks before putting systems on the network again. Part of these tips are explained earlier in this document (see the DataLabs section) but additional steps can include restoring with network access disabled for a final verification of data integration.

Restore options: depending on the situation, an entire VM recovery could be the best option. In other cases. a file-level recovery may be preferred. Familiarity with your recovery options in advance will help greatly in selecting the optimal recovery method and in reducing time to resolution.

Restore safely: as explained earlier, Veeam Secure Restore will trigger an antivirus scan of the image before the restore completes. Use the latest anti-virus and malware definitions, and perhaps leverage additional tools (i.e., more complete scanning) to ensure that a threat is not reintroduced into your production environment.

Hardening a backup infrastructure: valuable during recoveries

From a ransomware resiliency perspective, the Veeam Backup & Replication server is a critical part of the solution. It is important that there be as much separation as possible from production and the backup solution to provide ransomware resiliency. Here are some of the most important techniques to consider for these implementations:

Veeam servers without internet access: keeping backup servers isolated without being connected to the internet is a very important technique to protect against threats being introduced or propagated. If Veeam Cloud Tier or Veeam Cloud Connect are used, special consideration should be given to provide explicit access to cloud resources.

Accounts used for Veeam deployment: The most resilient approach would be to have as much separation as possible between accounts that are used for Veeam deployments. Consider connections to Veeam backup proxies, repositories, WAN accelerators and other components as an explicit account to map for required permissions. Some organizations may prefer a set of isolated accounts (i.e., non-domain) to be used for these components. Other organizations may prefer a separate Microsoft Active Directory domain for Veeam and related infrastructure tools that are as separated as possible. A specific recommendation is not to have shared accounts in-use across production data sources and the backup infrastructure. The worst practice here would be to have everything logged in as DOMAIN\Administrator, and to give that account permissions for key infrastructure resources such as Veeam, vSphere and Hyper-V. If that account is compromised, and if it was used through Veeam components, many resiliency techniques would be at risk.

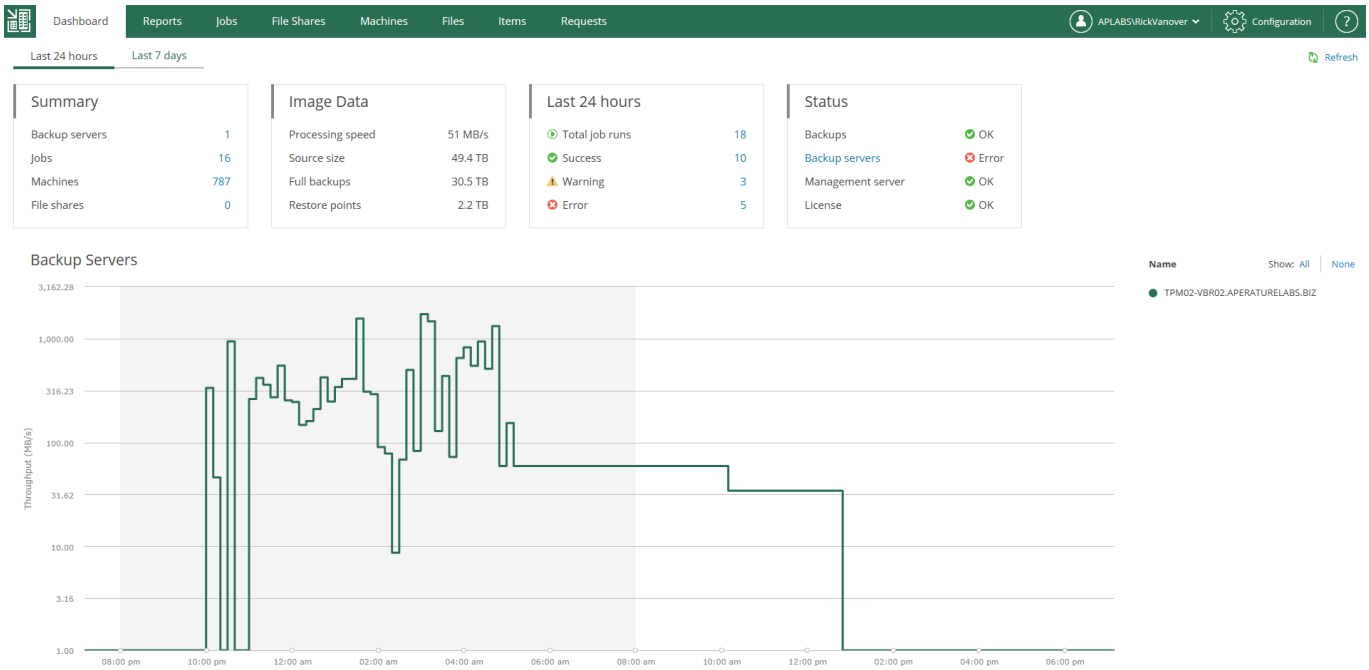
Recommended reading:

The required permissions for all Veeam products are thoroughly documented (as well as port requirements for each role) at helpcenter.veeam.com

Additionally, you may want to check the Veeam best practices guide on infrastructure hardening.

Setting explicit repository access: taking the previous recommendation one step farther, the backup repository is the most critical storage resource when it comes to ransomware resiliency. For this Veeam component, it is recommended that you prohibit access and browsing capabilities throughout the organization since this could prevent backups being leaked out of the organization. Additional protection can be provided through micro segmentation and internal network firewalling of explicit permitted traffic and permissions to the required sources and targets.

Intentionally use Veeam Backup Enterprise Manager: by using Veeam Backup Enterprise Manager for relevant tasks, access to the main control plane of the Veeam infrastructure is significantly reduced. Common tasks such as file-level restores, whole VM restores, quick backups, job cloning, job edits, requesting active full backups and more can be done in Veeam Backup Enterprise Manager. The key powerful aspect of Veeam Backup Enterprise Manager is that it can do these actions across all Veeam Backup & Replication servers that are deployed in an organization, regardless of geographical location. The figure below shows the main screen for Veeam Backup Enterprise Manager:



An additional technique to reduce the frequency of logins to the Veeam backup server with full permissions is using built-in roles. These roles can be used with Veeam Backup Enterprise Manager as well as with Veeam Backup & Replication itself. Roles include restore operator, portal user and portal administrator. More information about roles can be found in the Veeam User Guide or the [Veeam Help Center.]

Beyond the framework and call to action

The steps in this guide detail the best way to prepare to handle a ransomware incident in a well-accepted framework: identify, protect, detect, respond and recover.

Each one of these framework functions needs the other to be successful, and they require disciplined implementation across the overall IT practice. From a backup perspective, it's clear that the only option you have when ransomware is introduced is to recover data. The best next step is to assess the functions of the framework and to align all practices, including backup, to the recommendations of the NIST framework and this guide.

Valuable options in times of disaster: service providers, systems integrators and more

One of the key values of Veeam is the absolute portability afforded by Veeam backups. Coupled with the unknown nature of a ransomware incident, you have incredible options when it comes to restoring to new target infrastructure, should that be required.

There is a vast list of Veeam Cloud and Service Providers (VCSPs) that can provide target infrastructures to restore to, as well as many other services to help drive a fast and successful recovery. This can be as easy as seeking a VCSP that offers Veeam Cloud Connect backups with Insider Protection, so a copy of data is out of band from threat actors. Additionally, systems integrators and other Veeam partners have services that help drive the successful resumption of operations.

Resources

Recovery from ransomware is critical because it poses a threat to every technology for which we are responsible. It is worth having discussions with your stakeholders now in order to set plans in place and get alignment on your cybersecurity framework.

Our mission statement at Veeam is to be the most trusted provider of backup solutions that deliver Modern Data Protection. This is more important than ever when ransomware threats come into play. Read this white paper to learn how to ensure reliable data recovery.

Find more information about Veeam ransomware resiliency with the following resources:

FREE trial: veeam.com/backup-replication-virtual-physical-cloud.html

Resource Library: vee.am/ransomwareseriespapers

About Authors

Edwin Weijdema is a global technologist for Veeam Software based in the Netherlands covering a global role within the product strategy team. He serves as a partner and trusted adviser to customers and partners worldwide bridging business and technology. Edwin has over 28 years of industry experience with a key focus on data management, availability and cyber security. A veteran vExpert, Cisco Champion and with several other certifications, he is also a crew member and blogger at www.vmguru.com.

Follow Edwin on Twitter @Viperian, LinkedIn @eweijdema or @veeam.

Rick Vanover (Microsoft MVP, Cisco Champion, VMware vExpert) is senior director of product strategy for Veeam Software. Rick's experience includes system administration and IT management, with virtualization, cloud and storage technologies being the central theme of his career recently.

Follow him on Twitter @RickVanover or @veeam.

About Veeam Software

Veeam® is the leader in backup, recovery and data management solutions that deliver Modern Data Protection. We provide a single platform for Cloud, Virtual, Physical, SaaS and Kubernetes environments. Our customers are confident their apps and data are protected and always available with the most simple, flexible, reliable and powerful platform in the industry. Veeam protects over 400,000 customers worldwide, including 82% of the Fortune 500 and 60% of the Global 2,000. Veeam's global ecosystem includes 35,000+ technology partners, resellers and service providers, and alliance partners and has offices in more than 30 countries. To learn more, visit www.veeam.com or follow Veeam on LinkedIn @veeam-software and Twitter @veeam.

VEEAM

NEW V11

Eliminate Data Loss
Eliminate Ransomware

#1 Backup and Recovery

Try now:
https://www.veeam.com/backup-replication-virtual-physical-cloud.html