Beat ransomware: Education, Implementation and remediation with Veeam

Rick Vanover

Senior Director, Product Strategy

Veeam Software

Contents

State of the threat

The threat posed by ransomware can be seen on a grand scale, like in a news event about an outage at an organization. A recent article from ZDNet reports that ransomware attacks are getting bigger and are going to get worse.[1] Organizations need to take a marked focus to acknowledge this threat and take steps to prepare, defend and remediate. This is a critical step to take now to avoid an unplanned and likely ineffective response later during a ransomware incident.

When I talk about ransomware at events, I will often ask for a show of hands of how many attendees have had some sort of ransomware incident. It's shocking how many hands are raised. If you haven't had an event yet, you are lucky. Let's share some information to help you keep your data safe in the event of a ransomware incident.

[1] Via ZDNet https://www.zdnet.com/article/the-ransomware-crisis-is-going-to-get-a-lot-worse/

The three ultimate strategies for ransomware resiliency

If you want to win a ransomware battle, here are three strategies you can use to make sure you have the resiliency you need: **Education, implementation and remediation.**

Each of these strategies are their own disciplines with an ongoing need to constantly re-assess and adjust implementations to increase resiliency. Each area also will have their own disciplines, tools and, in many IT organizations, different personas that need to be involved. The successful resiliency approach is one that embodies the IT organization, supported by management. The rest of this paper will be aligned to these three strategies with practical Veeam technology tips as well as broader IT techniques that will give you what you need to implement resiliency for today and beyond.

Many individuals who've survived a ransomware incident have specific feedback on what could have been done to either prevent the occurrence or make recovery quicker. This will also be incorporated in this paper and made into tips that can be broadly implemented.

Education

The education journey starts after the risks of the threat actors are identified. This should be motivation enough to implement IT practices that will help you avoid being in a reactive position should a ransomware incident be the unplanned topic of the day.

There are two major audiences that should be targeted from an education perspective: IT staff and organizational users. It's important to target both groups, since threats can be introduced from both personas. It is reported that as of Q4 2019[2], over 57% of ransomware attack vectors were via a remote desktop protocol (RDP) compromise, over 26% were via phish attacks and over 12% were from software vulnerabilities.

Education through identifying attack vectors

From an education perspective, knowing that RDP, phish and software updates are the three main mechanisms for entry is a huge help in focusing the scope of where to invest the most effort to be resilient against ransomware from an attack vector perspective.

Most IT administrators use RDP for their daily work. In the later section about Veeam implementation, account separation will be mentioned for backup components. For RDP access, this is an opportunity to refine security access with this powerful entry point. It is hard to imagine that in today's IT world there are still many RDP servers that are directly connected on the internet. The reality is, internet-connected RDP needs to stop[3]. IT administrators can get creative with special IP addresses, redirecting RDP ports, complex passwords and more, but the data doesn't lie. The fact that over half of ransomware comes in through RDP tells us that exposing RDP to the internet does not align with a forward-thinking ransomware resiliency strategy. Later, we'll share some specific RDP recommendations to help you increase ransomware resiliency.

The other most frequent mode of entry is through phish mail. We've all seen emails that just don't make sense or look right. The right thing to do is delete that item, but not every user handles these situations the same way. There are two popular tools to assess the threat risk of phish success for an organization: Gophish and KnowBe4.

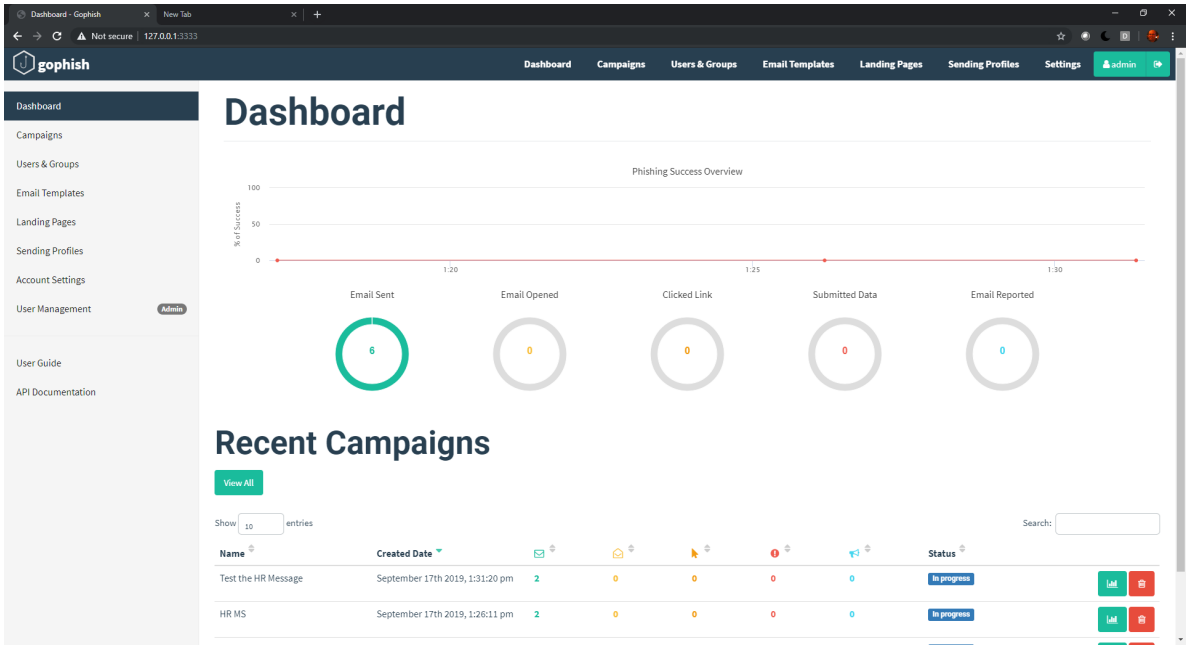
KnowBe4 (https://www.knowbe4.com) can be used for security awareness that goes beyond end user and administrator education. This service is a provides security awareness training with the added benefit of simulated phishing attacks.

Aside from KnowBe4, there are open-source resources in place to help with phishing as well. One example is Gophish (https://getgophish.com/), which allows you to create dashboards and send emails to see if your recipients will actually click on phishing emails. You can set up a phish test in just minutes.

Once the campaign is sent, you have some visibility into how many emails were sent, how many were opened, how many users clicked the link and more. This is a great way to easily test the training levels of users in your organization. The Gophish dashboard is shown below:

[2] Via Coveware report: https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

[3] Via ESET https://www.welivesecurity.com/2019/12/17/bluekeep-time-disconnect-rdp-internet/



These tools can be effective in measuring an organization's competency in being able to self-assess the risk of phishing emails, attachments and more.

Another factor that comes into play is the risk of exploiting vulnerabilities. Keeping systems up-to-date is an age-old IT responsibility that is more important now than ever. While this isn't a glamourous task, it's a good investment, should another ransomware incident exploit a known and patched vulnerability. Also, keep in mind the need to stay current with updates to critical categories of IT assets: Operating systems, applications, databases and device firmware. There have been several ransomware strains based on older discovered vulnerabilities that have since been corrected. Examples of this include WannaCry, Petya and Sodinokibi[4]. These vulnerabilities also include non-operating system services, such as njRAT[5] which applies to Adobe Flash.

It is also recommended that you take the same aggressive stance on updates to endpoints as well. As an attack vendor, endpoints can be just as much of a risk as data center systems, especially for threats that like to dwell to gather target information. This dwell time averages around three days[6].

Education through preparation

There are several additional preparation steps to take, like learning how to use the tools you have in place. For example, if there is a ransomware incident and restoring data is the right course of action, IT organizations can be more prepared by becoming familiar with different restore scenarios. This can give IT professionals familiarity toward the process, a reasonable expectation of how much time is involved and most importantly, confidence in that the process will work. A few examples of these educational practice steps are summarized below:

[4] Via ZDNet https://www.zdnet.com/article/sodinokibi-ransomware-is-now-using-a-former-windows-zero-day/

[5] Via TrendMicro https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/lord-exploit-kit-rises-delivers-njrat-and-eris-ransomware

[6] Via ZDNet https://www.zdnet.com/article/most-ransomware-attacks-take-place-during-the-night-or-the-weekend/

- **Veeam secure restore:** During secure restore, Veeam Backup & Replication™ mounts the disks of the machine that you plan to restore. Then, Veeam Backup & Replication triggers an antivirus to scan files from these mounted disks. If the antivirus detects malware during the scan, Veeam Backup & Replication will either abort the restore process, restore the machine or restore its disks with restrictions that depend on secure restore settings. This is a small step in the restore process, but it can give you some extra confidence to not re-introduce a threat based on newer definitions.
- **Veeam DataLabs™:** A Veeam DataLab is a SureBackup® job that takes a virtual machine (VM) backup and powers it on in an isolated environment. This functionality is intended to verify that a system is indeed recoverable, but it can also be used for tests like updates to applications or the operating system. DataLabs can be used to take a restore point and ensure that the system functions as expected before restoring. An additional use case is to power on one or more systems in the DataLab without network access to perform some potential remediation activities.

  Generally, it is recommended that you're familiar with Veeam SureBackup. This can provide forward indication that a system may be unrecoverable due to a ransomware threat or many other scenarios. In a ransomware remediation situation, the SureBackup job could easily be run to ensure that the system can restore correctly and that applications will function as expected. You also have the option to leave SureBackup jobs running after they complete for a manual check to see if a ransomware threat exists in the system before restoring. More on Veeam DataLabs can be found in the implementation section of this white paper.

- **Multiple restore scenarios:** Depending on the type of incident, it may be advisable to do a different type of restore. For example, a replica failover may be the most logical way out of a ransomware incident. A file-level restore may make the most sense. Other scenarios may be more appropriately solved by whole VM or Veeam Agent restores. It is worth becoming familiar with all the different restore scenarios to help build confidence in successfully remediating a ransomware incident.

The education aspect must be taken seriously. Whether it is assessing the phish risk of an organization, removing the most frequent attack vectors or keeping systems and software up-to-date, taking these steps are essential. If these steps are not taken, ransomware risk is increased. One way to measure this investment in education is to compare it with the risks, costs and pressure of dealing with a ransomware incident unprepared.

In all situations, if a ransomware incident occurs, the only course of action is to restore data. From an education perspective, this mindset will dictate the seriousness of the subsequent sections of this paper that surround the implementation and remediation of Veeam backup products. Data loss is not an option, paying the ransom is not an option. Reliable recovery is the preferred outcome, and the following tips will provide resiliency for organizations in the threat scape.

Implementation

Veeam backup products are known for being simple, flexible and reliable. This is a great set of attributes for trying new capabilities. Regarding ransomware resiliency, implementing a backup solution is a lot like going through a compliance audit. A product is not necessarily compliant or non-compliant to a standard. Rather, compliance is completely dictated on how the product is implemented and audited. When it comes to a ransomware incident, resiliency is completely based on how the backup solution is implemented, the behavior of threat and the course of remediation.

As an important part of ransomware resiliency, implementing your Veeam backup infrastructure is a critical step. Implementation recommendations for ransomware resiliency are organized in the following sections:

- Protection of the Veeam Backup & Replication server and components
- Implementing Veeam capabilities for ransomware detection
- Ultra-resilient backup storage and the 3-2-1 Rule
- Multiple recovery techniques configuration
- Endpoint protection
- NAS protection
- Veeam encryption of backup data
- Orchestrated recoveries of backups and replicas

Protection of the Veeam Backup & Replication server and components

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

Veeam servers without Internet access: Keeping the backup server isolated without connectivity to the Internet is a very important technique to protect against threats getting introduced or propagating. 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 for 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 (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 separate 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.

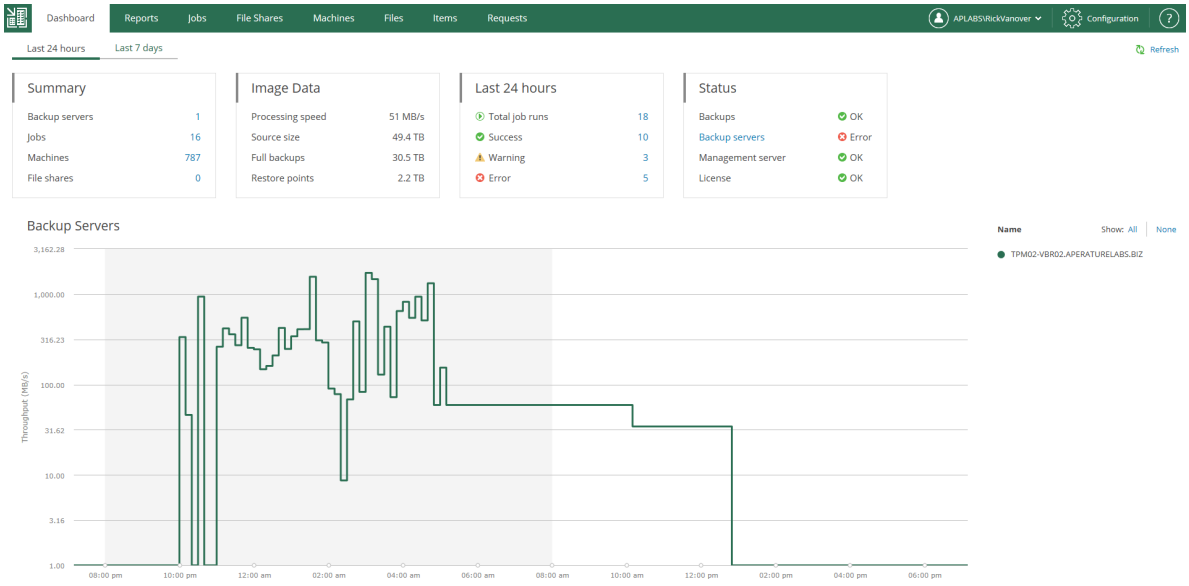
Recommended reading

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

Additionally, you may want to check the Veeam Best Practices Guide on infrastructure hardening: https://www.veeambp.com/infrastructure_hardening

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

Intentionally use Veeam Backup Enterprise Manager: By using Veeam Backup Enterprise Manager (BEM) 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 BEM. The key powerful aspect of BEM is that it provides these actions across all the Veeam Backup & Replication servers that are deployed in an organization. The figure below shows the main screen for BEM:



An additional technique to reduce the frequency of logging into the Veeam backup server with full permissions is using built-in roles. These roles can be used with BEM 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 (https://helpcenter.veeam.com/docs/backup/hyperv/users_roles.html?ver=100).

Require two-factor authentication for remote desktop access to Veeam: For the systems that are running Veeam Backup & Replication console roles, it is recommended that you require two-factor authentication to start a remote desktop (RDP) session. RDP in general is one of the most frequent attack vectors (57.4% of attacks originate from RDP7). Even on a network without internet access, this attack vector should be considered.

[7] https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

Popular approaches for two-factor authentication are native Microsoft tools or an external tool such as Duo.

Microsoft two-factor authentication for remote desktop services:
https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-plan-mfa

Duo multi-factor authentication
https://duo.com/product/multi-factor-authentication-mfa

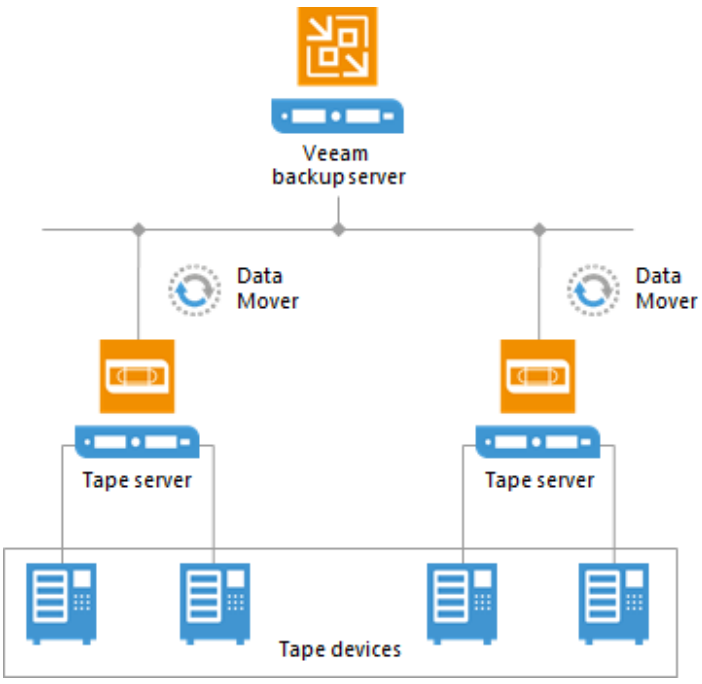
Ultra-resilient backup storage and the 3-2-1 Rule

If there is one key takeaway from this paper, it is to have a form of ultra-resilient backup storage. Ultra-resilient backup storage requires that you have one or more copies of backup data on the following media:

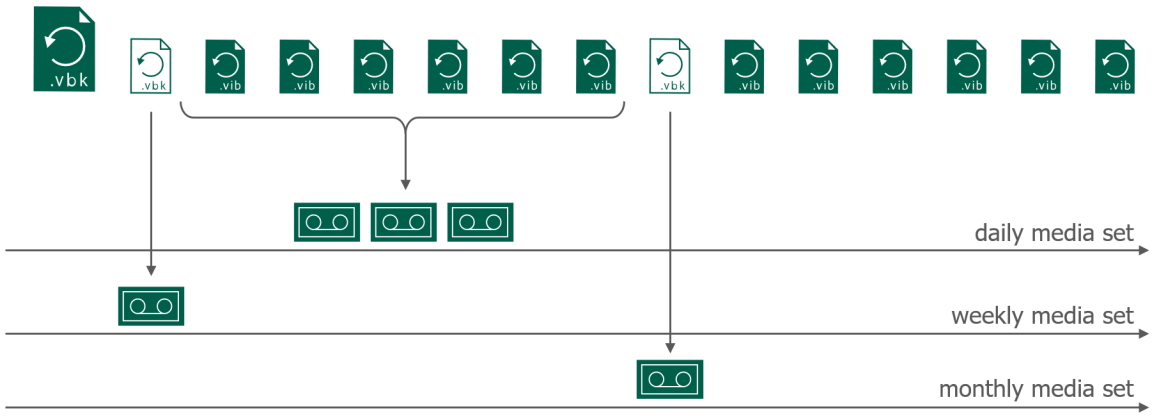
- Backups on tape
- Immutable backups in S3 or S3-compatible object storage
- Air-gapped and offline media (i.e., removable drives, rotating drives)
- Backups in Veeam Cloud Connect with Insider Protection

Backups in an ultra-resilient storage type will be one of the most critical defenses for ransomware resiliency. Each characteristic and each organization should select which approach makes the most sense for the specific situation. Beyond ransomware, these options can bring other protection techniques for backup data resiliency such as mitigating insider threats and accidental deletion. Each of these ultra-resilient media types are explained below:

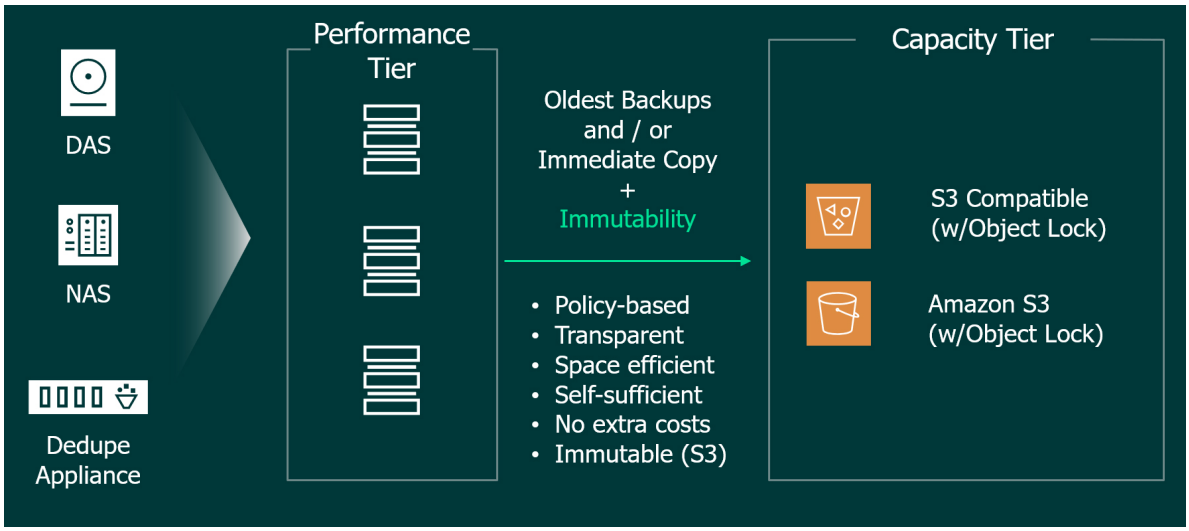
Backups on tape: Every IT organization has their own opinion on tape media, but there is no doubt that the acquisition cost, offline capability and portability of tape is hard to beat. Tape media that's ejected or out of a library is automatically offline unless it's being written to or read from. Veeam supports write once read many (WORM) media for additional resiliency against ransomware. Veeam also has broad tape media support, including writing files to tape and complete backups on tape. Veeam tape support for VM and physical server backups is visualized in the simple mode below:



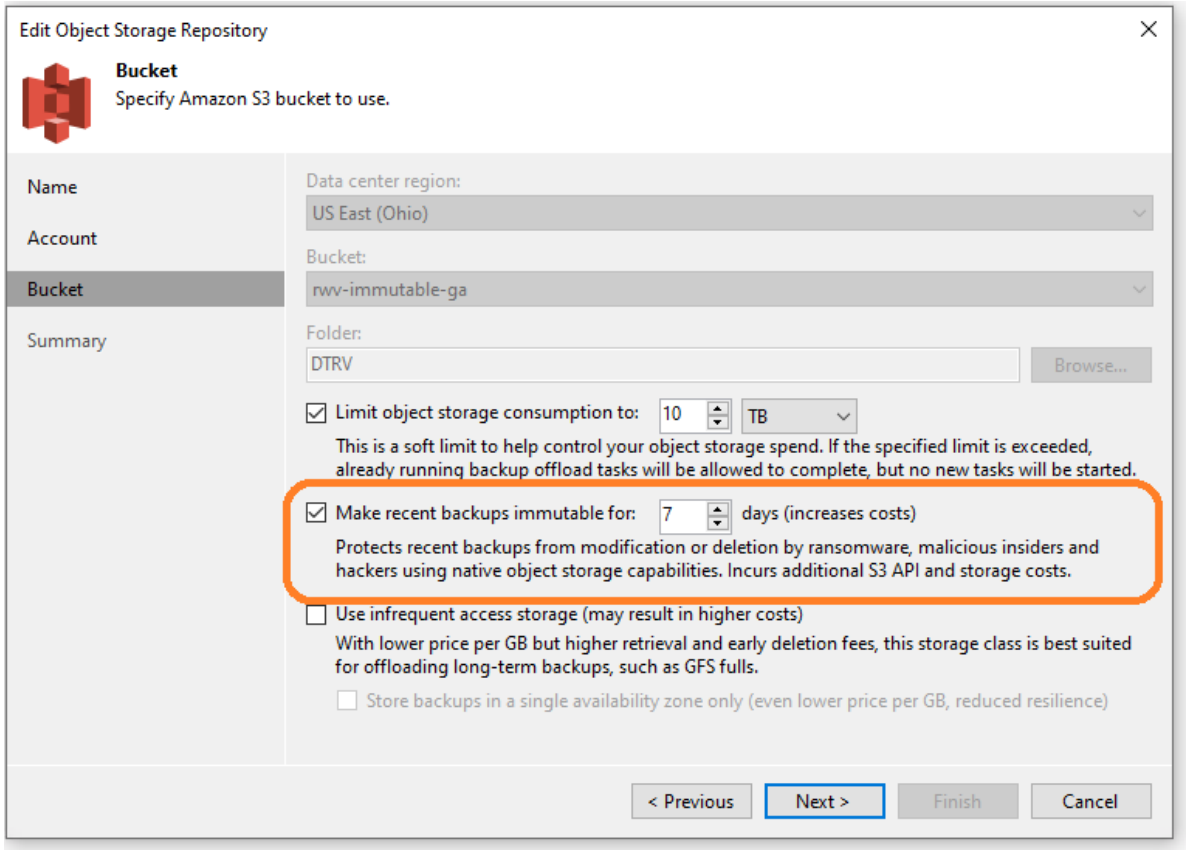
Tape support in Veeam is flexible for most configurations of modern LTO tape devices and libraries. There are several ways that tape support can be used to bolster ransomware resiliency. One of those ways is to only put a fixed amount of data over a shorter amount of time on tape media, such as a few 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 restore points. Media sets in Veeam are visualized by the figure below, which shows a sample daily, weekly and monthly media set:



Immutable backups in S3 or S3-compatible object storage: Veeam Cloud Tier supports immutable backups as a powerful technique to become resilient against ransomware and other threats. This is achieved by leveraging Veeam Scale-out Backup Repository™ (SOBR) with capacity tier enabled (this is also known as the cloud tier). The capacity tier is a policy-based capability that writes backup data into object storage. IBM Cloud, Azure, AWS and AWS S3-compatible object storage targets are supported, however only the public AWS S3 and select S3-compatiable storage systems support the object lock with compliance mode that's needed for Veeam backup data to be placed in a bucket as an immutable backup.



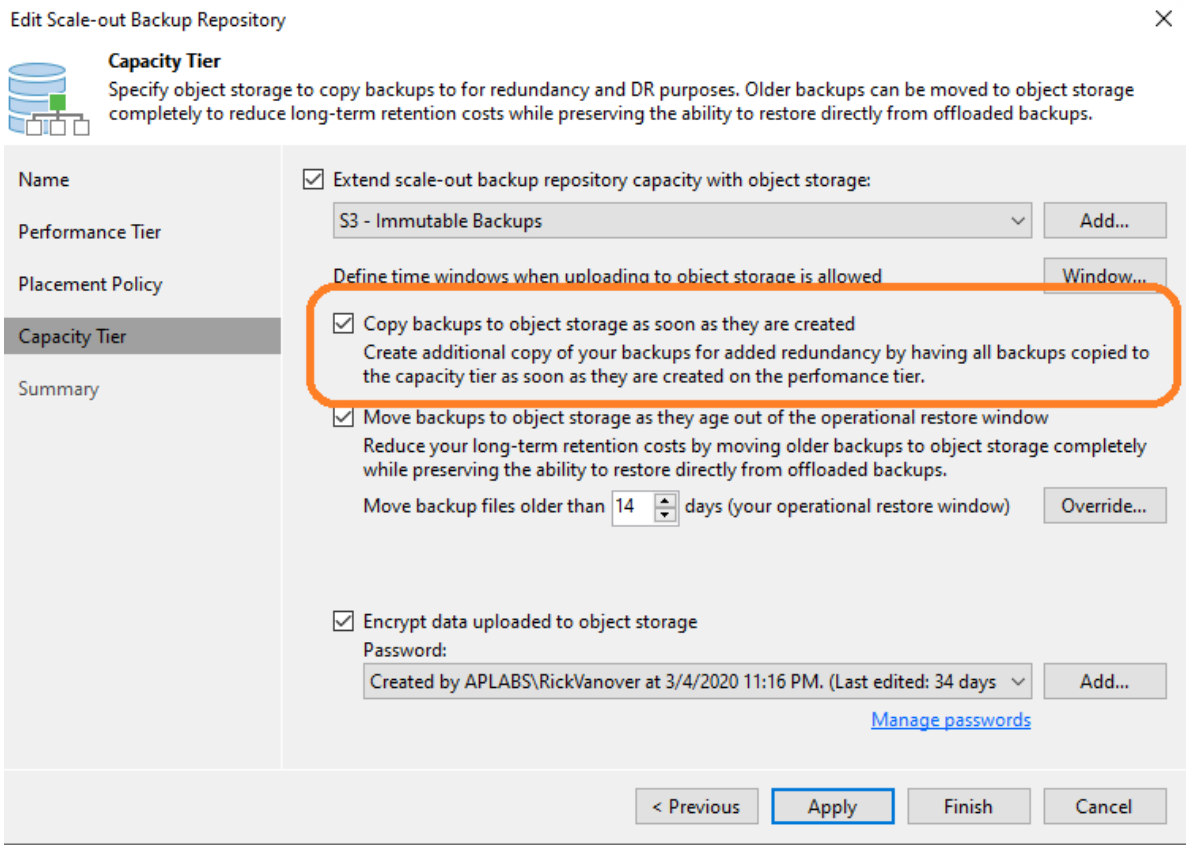
The wonderful aspect about S3-immutable backups is that it could not be easier to configure within Veeam Backup & Replication. There are two properties that should be configured for the most resilient usage of Veeam Capacity Tier. The first is the AWS S3 or S3-compatible bucket which should select the option to make backups immutable for a specified number of days. This applies to all backup data going into the bucket from the Scale-out Backup Repository tiering process that happens either after a backup is completed (copy mode) or after an interval (move mode). Setting the immutability period on a bucket is shown below:



The described immutability setting is a property for the object storage bucket. To most effectively use object storage to be resilient against ransomware, an additional setting should be used as a property of the Scale-out Backup Repository. Capacity tier object storage will then receive backup data by moving backup data to object storage for backup files that are older than a specified operational restore window (say 14 days or older). There is also an option to copy backups to object storage as soon as they are created (i.e. copy mode).

Copy mode is an important additional step in being resilient against ransomware, as it will immediately make a copy of the backup data in object storage after a backup job is completed. As the backups age, the move mode will still remove, or tier, the backup data from the on-premises extents in the performance tier. In the time between backup creation and the operational restore window, the backups will exist both on-premises and in object storage. Couple that with the immutable setting, and there is a strong ransomware resiliency technique in place.

This is important as in many cases, restores from the most recent points are most desirable, because they have the nearest recovery point objective (RPO). Configuring copy mode for the Scale-out Backup Repository is shown in the figure below:



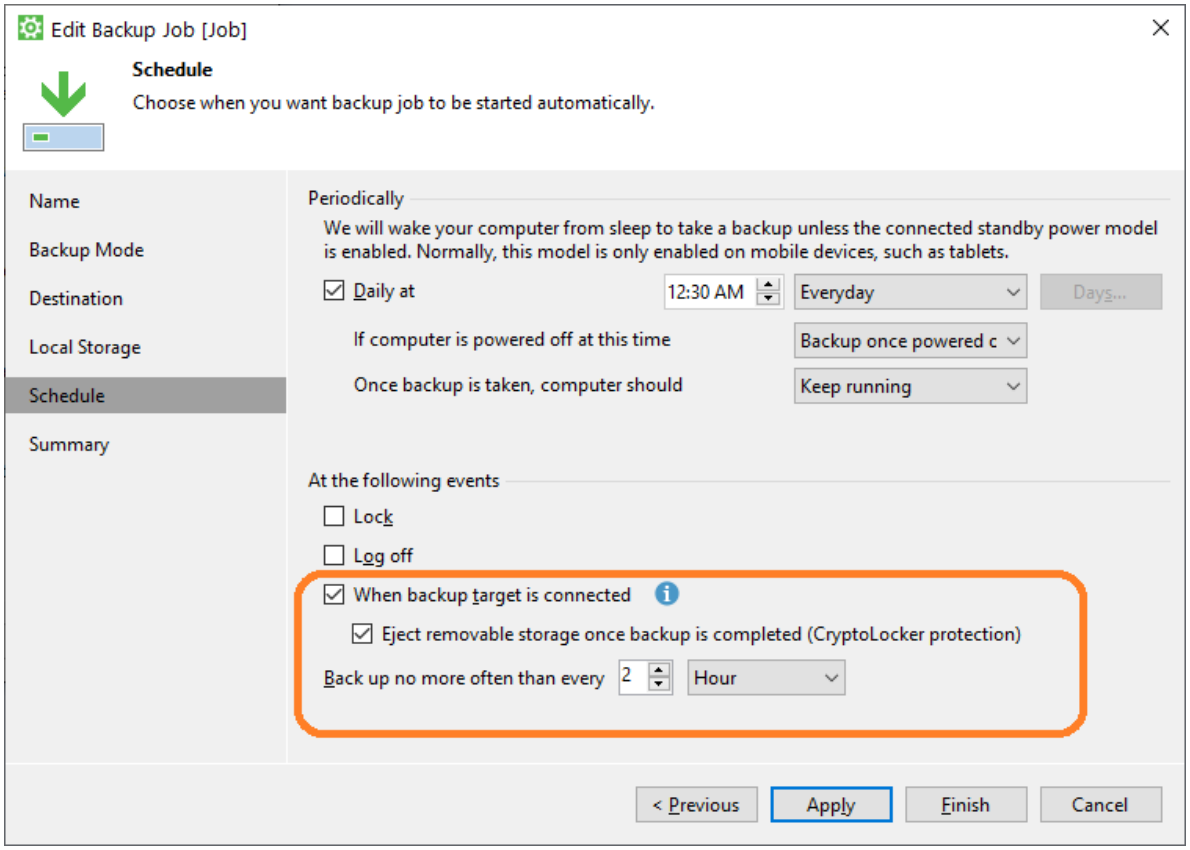
The option to encrypt backup data in object storage is also shown in the figure above. It goes without saying that this is a recommended configuration for backup data in the cloud.

Recommended reading

You can read more about the immutable backup capability of Veeam at http://vee.am/s3immutable

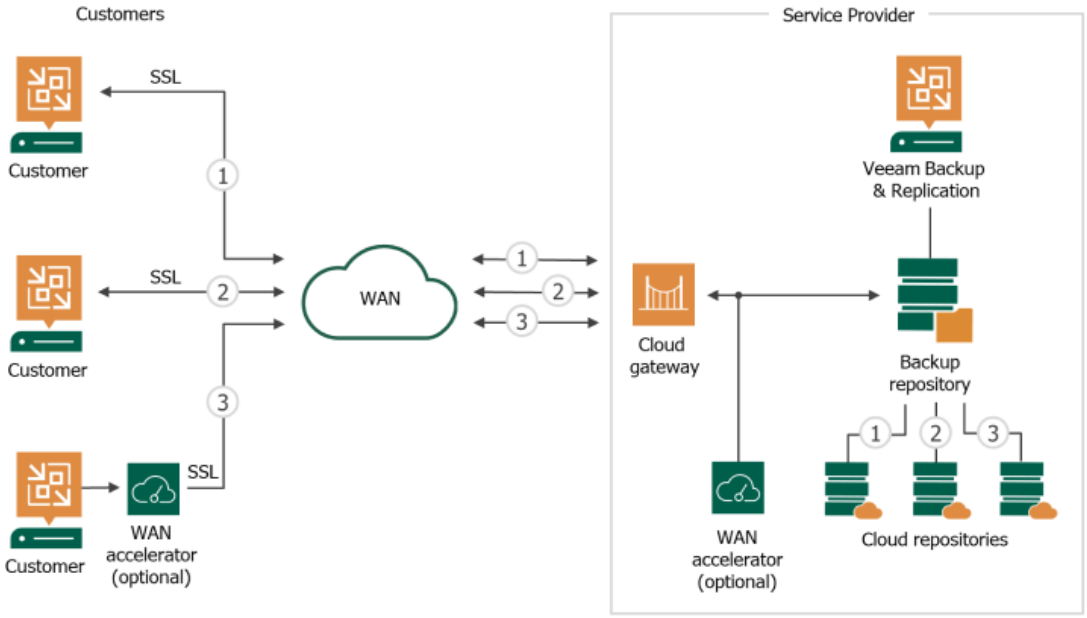
Air-gapped and offline media: Rotating drives and removable drives are other media types that have offline characteristics like tape. For larger data profiles, this becomes somewhat harder to manage since single drives that can come offline are generally limited by drive sizes (although these sizes are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

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



Backups in Veeam Cloud Connect with Insider Protection: Veeam Cloud Connect is an established technology in the market 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 provided 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 to 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 is retained by the service provider and can be exposed by intervention, such as a support call. This process will allow backup data to be re-populated into the Veeam Cloud Connect repository to 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: http://vee.am/splookup

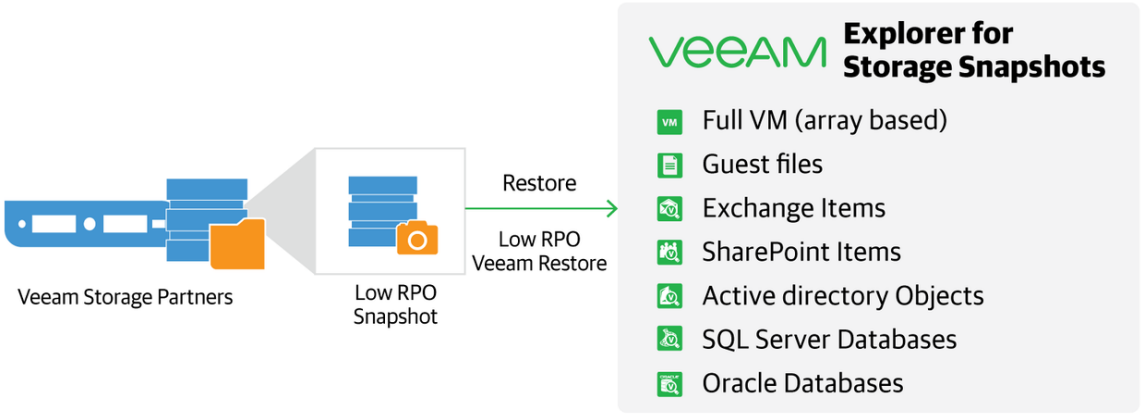
The 3-2-1 Rule: For many years, Veeam has advocated for the 3-2-1 Rule as a general data management strategy. The 3-2-1 Rule recommends that there should be at least three copies of important data, on at least two different types of media, with at least one of these copies being off site. The wonderful 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.

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 for becoming resilient against ransomware.

Multiple recovery techniques configuration

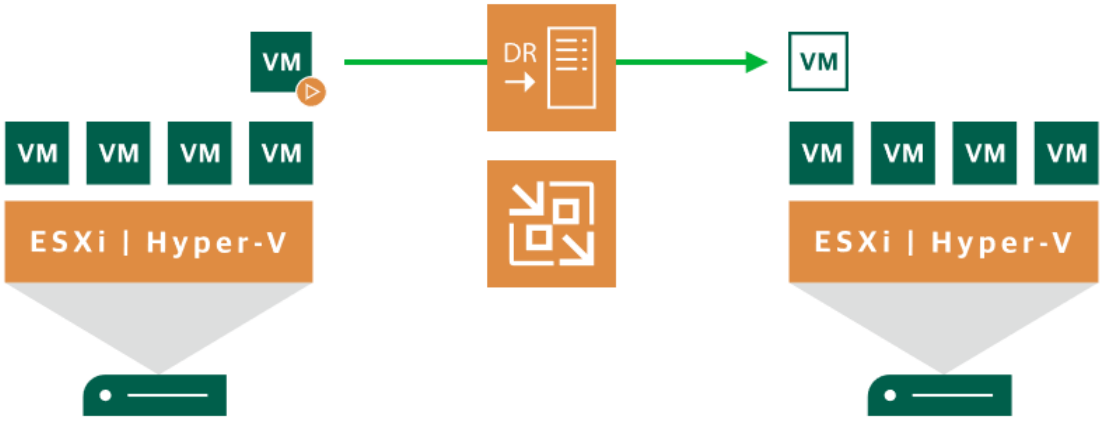
In the process of implementing Veeam Backup & Replication, you inherently connect to various other systems. These systems include virtual environments like VMware vSphere, Microsoft Hyper-V or Nutanix AHV, physical environments such as Windows, Linux, AIX and Solaris and storage array systems. The practical advice in this situation is to have all recovery options available at your disposal. The most popular type of restore process usually involves a whole system (i.e., VM or server) recovery, file-level recovery or application-level recovery. A few recommendations beyond the most popular restore types are explained below:

Storage Snapshot integration: If a primary storage system is in use with a Veeam-integrated storage snapshot support, this can be an incredibly versatile high-speed recovery technique. Veeam Explorer™ for Storage Snapshots can quickly recover VMs from storage-level snapshots that are taken on a schedule. Veeam Explorer for Storage Snapshots is visualized in the figure below:



The technique above is having production data (i.e., VMs) to be able to drive a restore technique from a primary storage snapshot. However, it is also recommended that you back up off the primary storage system. Veeam also supports read-only Storage Snapshot techniques such as NetApp SnapVault and Pure Storage SafeMode snapshots.

Veeam replication: Many organizations come to Veeam for backup and recovery of critical workloads, but the replication engine is a powerful technique that can be part of ransomware remediation. Having replicated VMs to the same same site or to a disaster recovery (DR) site is a high-speed recovery technique that can help quickly eliminate a threat. A simplified view of a Veeam-replicated VM is illustrated below:



Keep in mind that replication may be a scenario in which ransomware may have exposure on the target side as well. A few key considerations for replication in general regarding ransomware resiliency include:

- Using different security contexts on both source and target sides with hypervisors and management software, like vCenter or System Center.
- Restore points for replicas are much like the backup engine and represent the VM at the time the replica job ran.
- For VMware environments, SureBackup jobs can be made for Veeam replicas to ensure that a replica powers on and functions as expected before restoring from a ransomware incident.

Another Veeam product, Veeam Availability Orchestrator, delivers a reliable, scalable and easy-to-use orchestration and automation engine that's purpose-built for today's business continuity/disaster recovery (BCDR) needs. By eliminating manual testing and recovery processes that are inefficient, lengthy and error-prone, Veeam Availability Orchestrator provides a planned, practiced and proven DR strategy – using replicas and backups – for more resilient IT operations. Veeam Availability Orchestrator also will ensure that replicas and backups will meet recovery time objectives (RTOs) and RPOs automatically, which can give incredible confidence to a comprehensive DR strategy and provide proof that your availability SLA can be met. In the context of ransomware resiliency, having confidence in DR can be a powerful way to recover from a ransomware incident.

Many options: Depending on the nature of a ransomware situation, there isn't always a single way to recover. Whole VM or whole system recoveries in many cases are very effective, but it is advisable to have experts do other types of restores to potentially migrate the select data needed. This includes file-level recoveries, application-level recoveries or select drive recoveries, such as a VHDX or a VMDK file.

Endpoint protection

Many organizations know Veeam for data center backups for physical servers, virtual machines and more. But, Veeam Agents also provide backup for desktops, laptops and Windows tablets. For Linux and Windows backups of endpoints, organizations can add an additional level of ransomware resiliency to the endpoint.

The strategy for endpoint backups at face value provides a ransomware resiliency technique to recover from backups in the event of an incident. There are additional benefits to this as well when the Veeam Data Integration API is considered for endpoint backups. There is also an opportunity to do post-backup scans of endpoint systems to shorten the time between when a threat comes into a system and the start of an exploit.

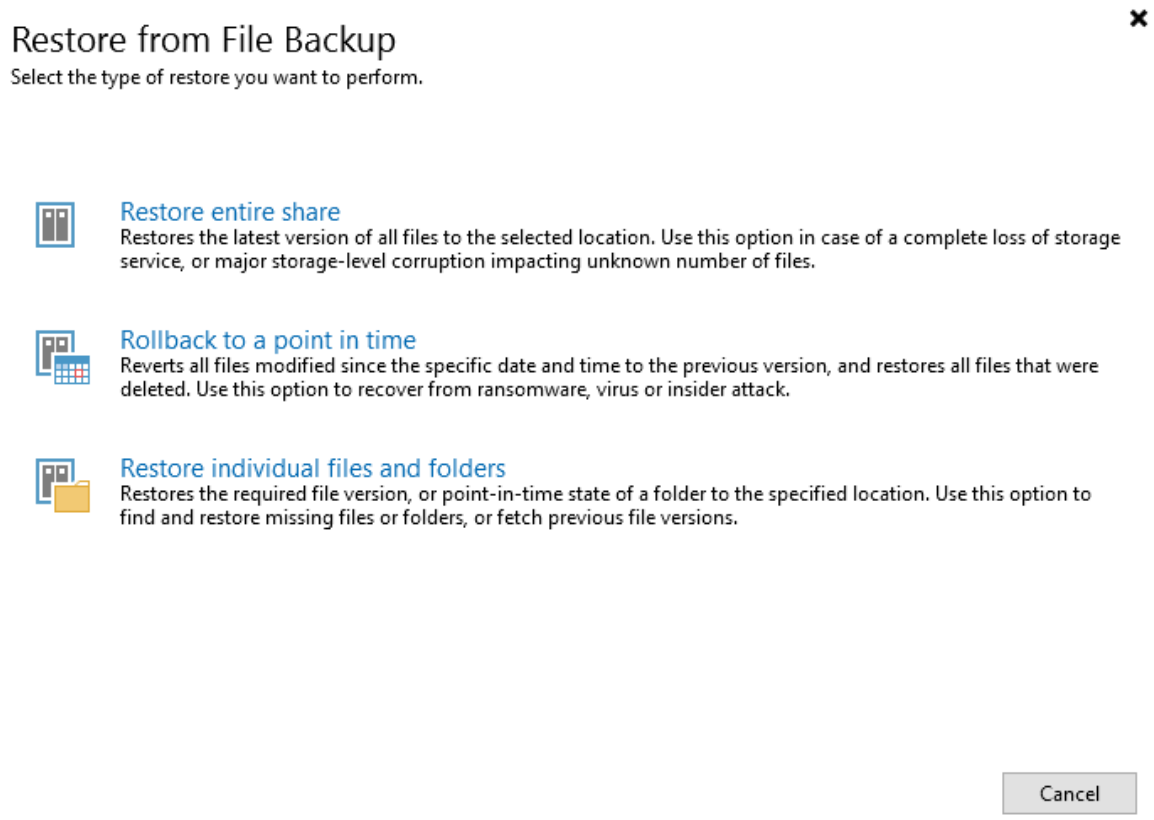
As mentioned earlier, Veeam Agent *for Microsoft Windows* supports ejecting removable media to make it offline through two critical ransomware resiliency techniques. The first is just having a backup and the second is having a backup be offline. This is supported by Linux systems as well as desktops, laptops and Windows tablets.

NAS protection

NAS systems are also a frequent target of ransomware attacks. Coupled with insider threats or accidental deletion, there are many reasons as to why file data needs to be considered as 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 three 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 the specified restore point. The third recovery scenario is to restore the entire share to a new device for a loss-of-device scenario.

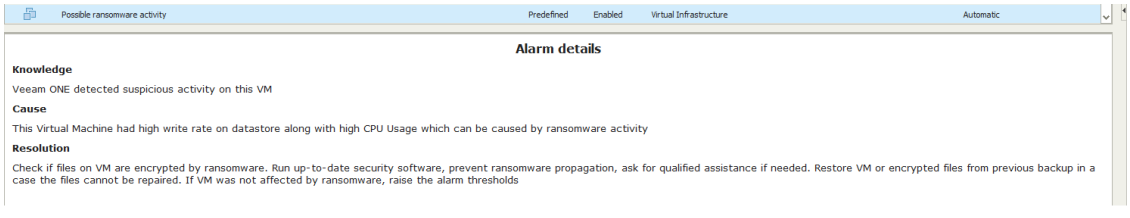
Each scenario has a ransomware use case for recovery, but the second scenario provides a compelling way to recover a share if a ransomware incident has occurred. If the threat is removed but part of the NAS share has been encrypted or deleted, this restore type can take the contents of the share back to what it was at the time of the specified backup. 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 is to make a 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:



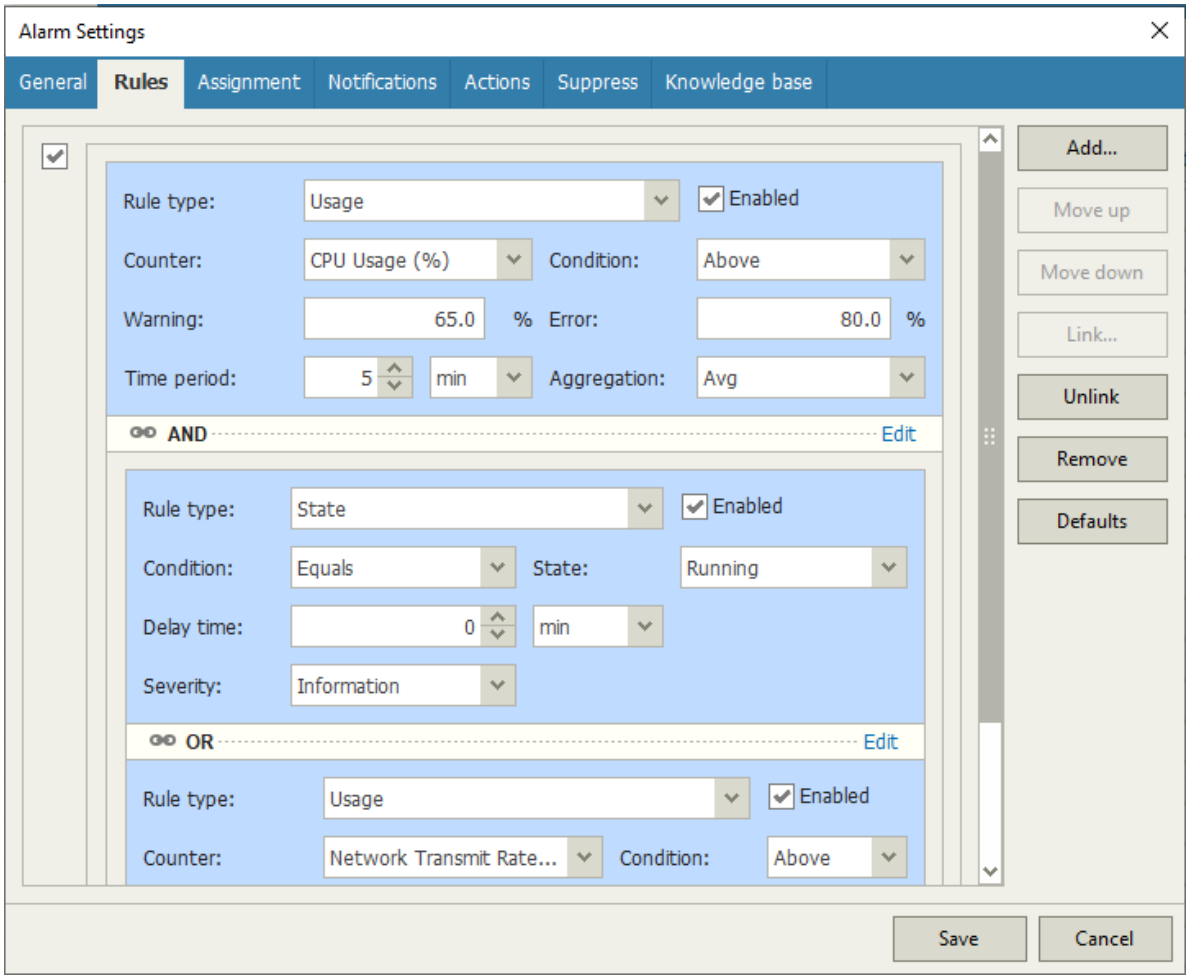
Implementing Veeam capabilities for ransomware detection

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

Possible ransomware activity alarm: This Veeam ONE™ alarm will detect a combination of high CPU activity along with sustained write I/O on a drive. This alarm is shown in the figure below:

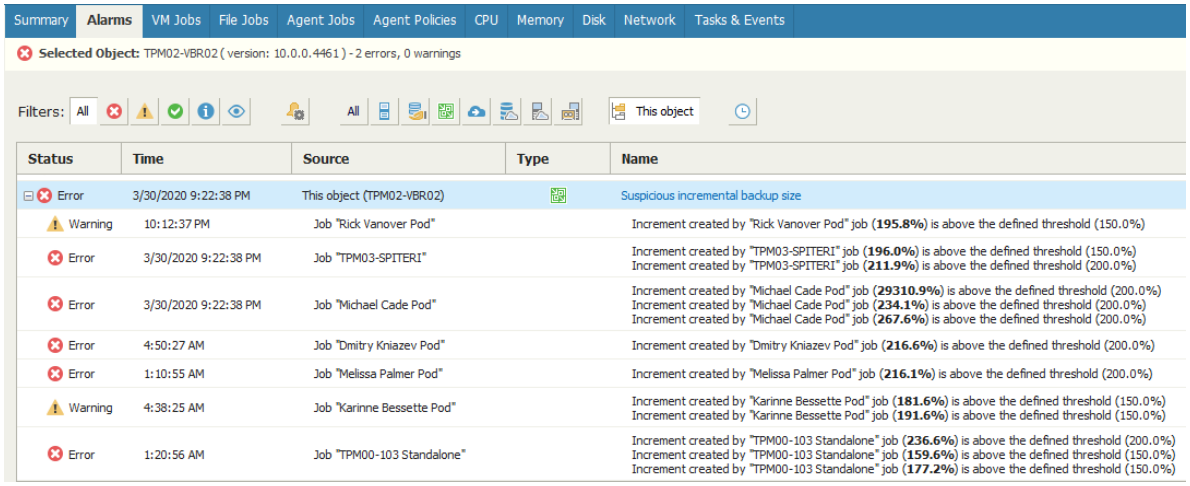


This alarm is customizable as well. The defaults are a good starting point for possible ransomware activity, but they can be adjusted to be more conservative in what triggers this particular alarm. This customization is shown in the figure below:



For organizations that are use Veeam ONE, the next piece of advice is critical in addressing what happens when this alarm is triggered. I recommend some specific actions that are built-in to the alarm that do more aggressive notifications to IT staff. This includes SMS messaging, alerting security teams and even extreme steps like powering off a VM or disconnecting the network interface via the actions step on the Veeam ONE alarm. If you have both VMware and Hyper-V systems in place, be sure to make these actions required for both environments.

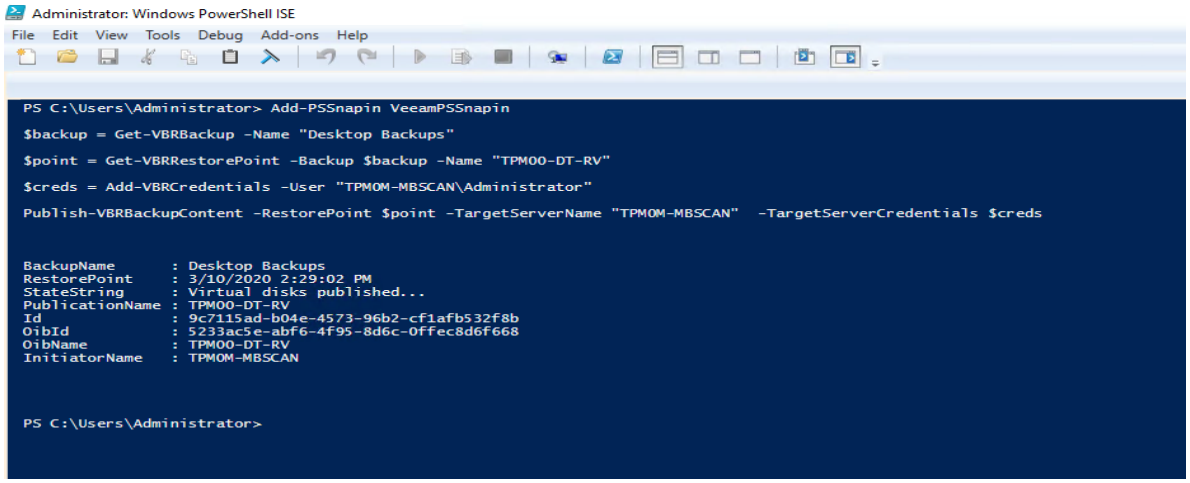
Suspicious increment size: This alarm applies to Veeam ONE when it is monitoring Veeam Backup & Replication in the data protection view. This alarm is a way to report that an incremental backup is suspiciously large. This logic is based on normal change rate and the possibility that the source data is 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 a150% change rate and an error alarm at a 200% change rate. This alarm is shown below:



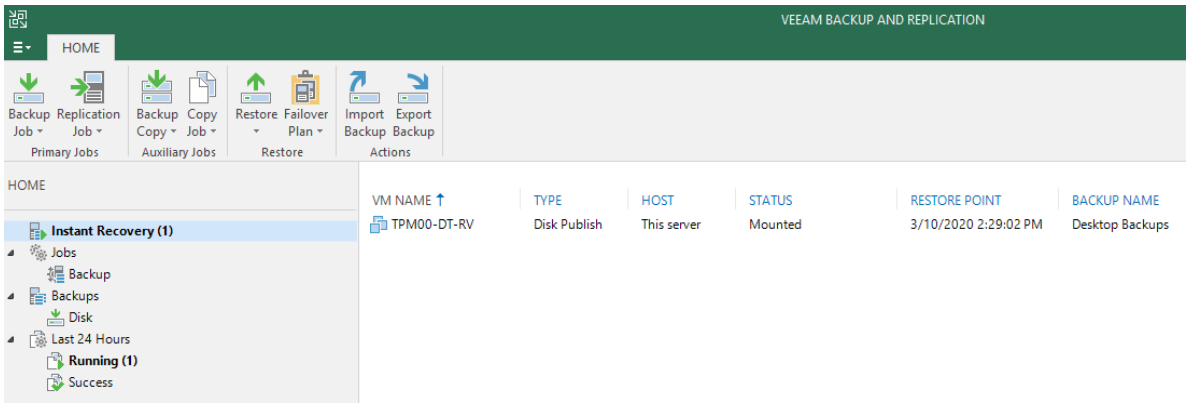
Data integration API: The Veeam Data Integration API is best consumed through PowerShell and is part of Veeam Backup & Replication v10. This capability allows the data of backup files to be exposed as a mounted Windows folder and it allows you access data that is available in the backup created by Veeam Backup & Replication. This capability is a great new technique 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.

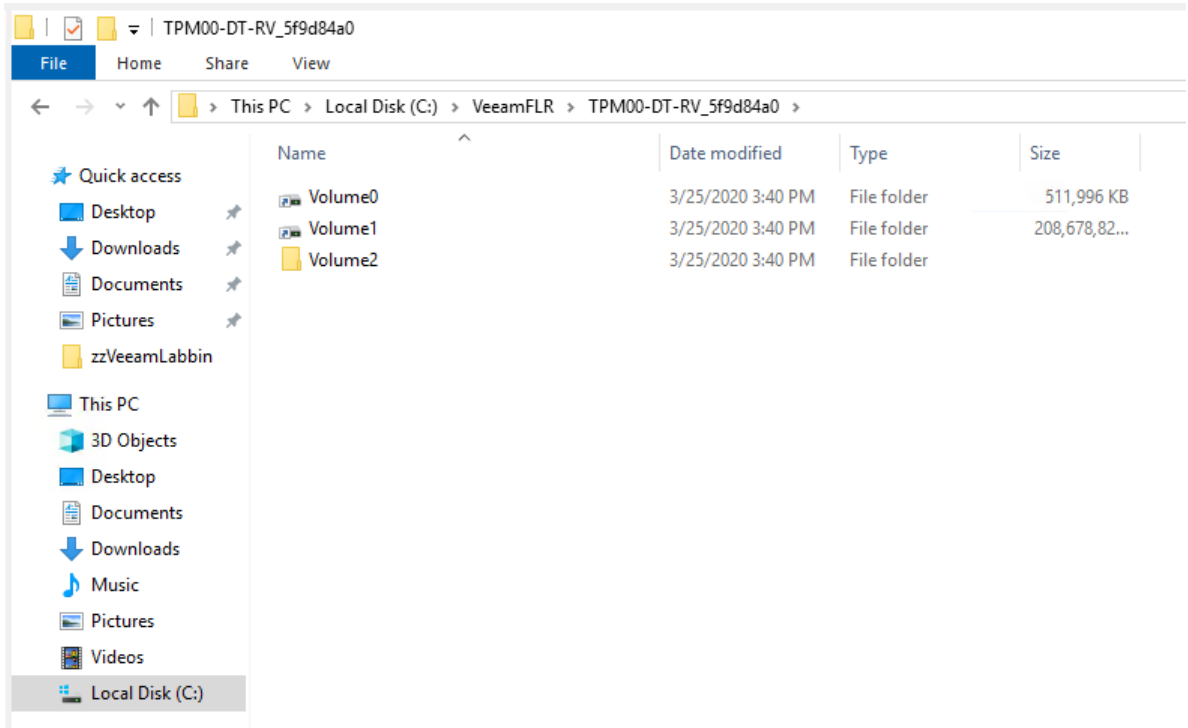
Using the data integration API will start with backups in a Veeam repository. The example PowerShell script will call the backup of a system (TPM00-DT-RV) to be mounted via the Publish-VBRBackupContent Cmdlet. This is shown in the figure below:



This is a sample PowerShell script for one backup being mounted, but multiple backups can be mounted with the Cmdlet. This will perform an instant disk publish task in Veeam Backup & Replication. This particular action is similar to an Instant VM Recovery®, 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. This publishing is done transparently through iSCSI from the Cmdlet. This Veeam Backup & Replication server shows the backup exposed as disk publish below:

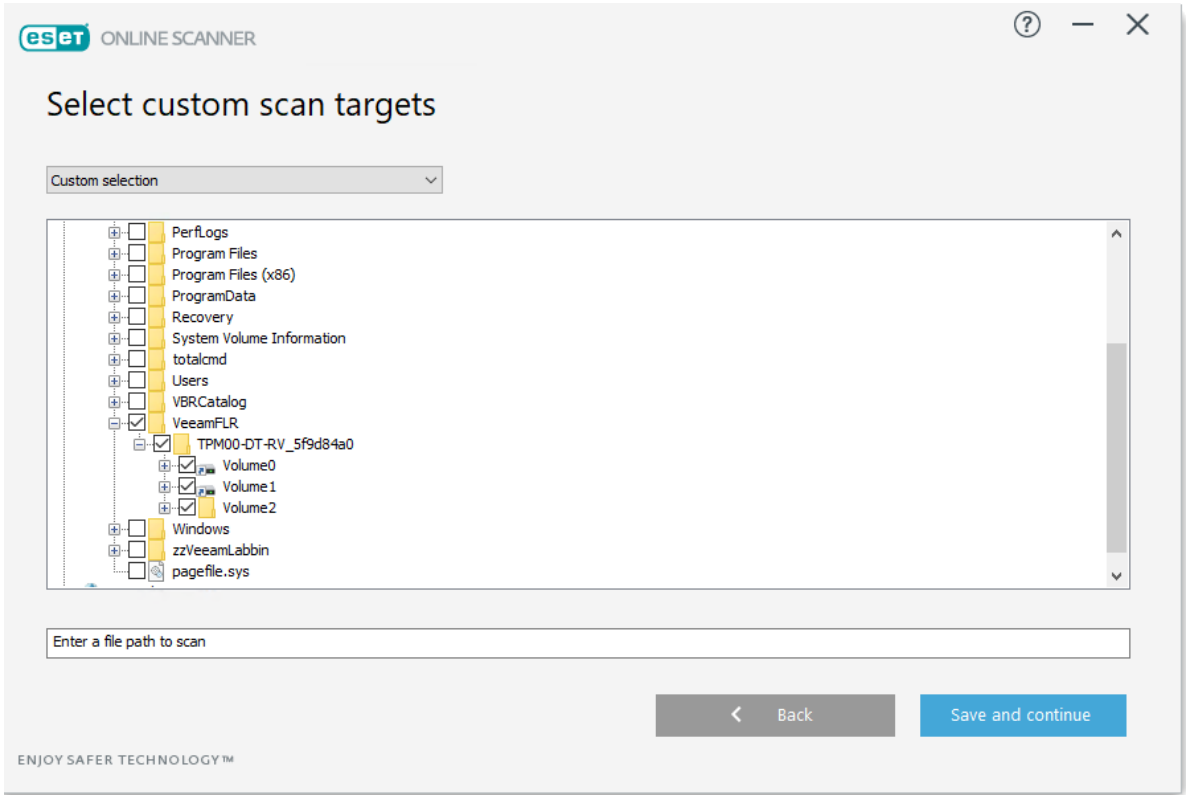


Once this is running as shown above, the contents of the backed-up drives are exposed like folders locally on the Veeam Backup & Replication server:

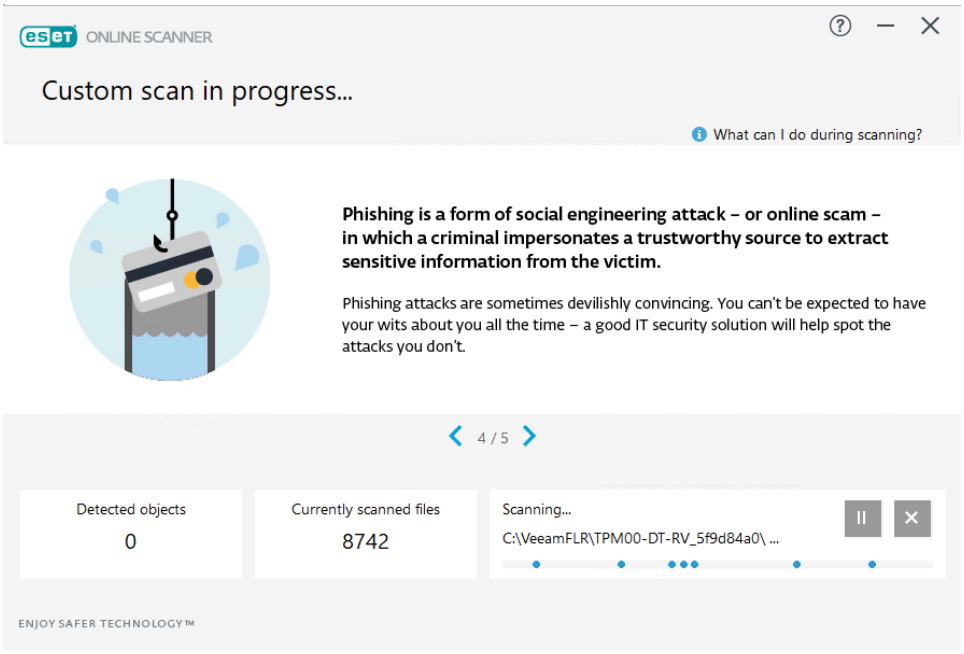


This is point at which you can unleash the power of your backup infrastructure. The systems that are backed up with Veeam then can have some advanced scanning performed on them. Two specific examples that can aid in detection that I'll summarize are using ESET scanning tools and Total Commander.

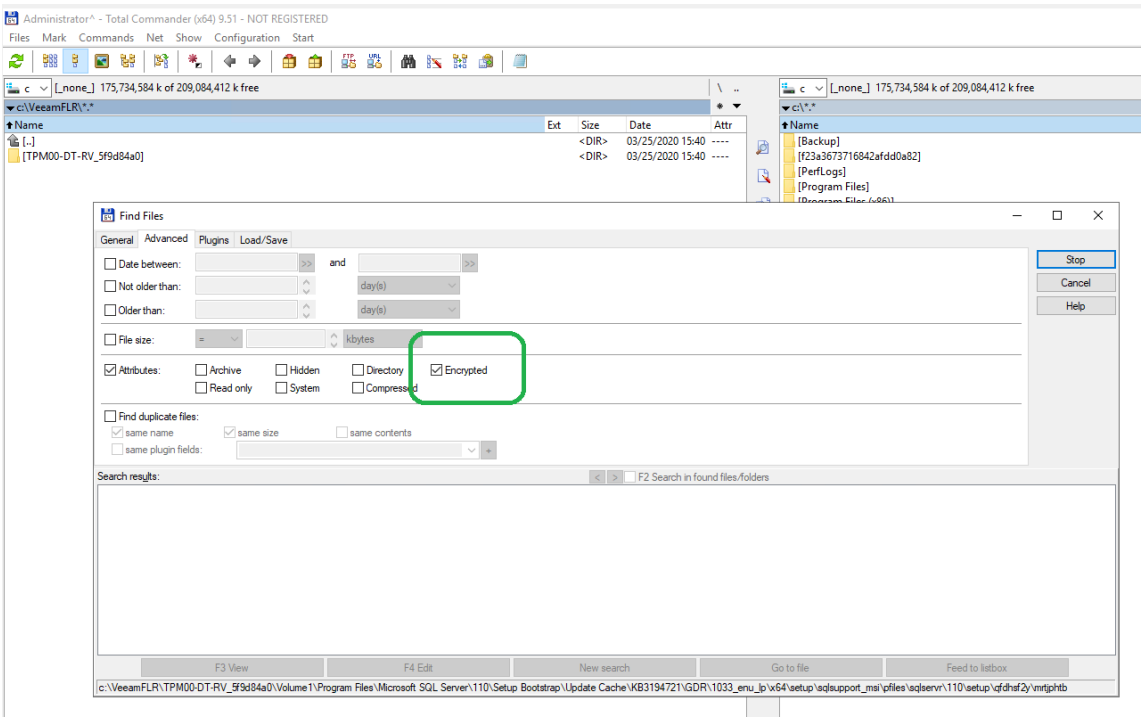
In the first example, ESET can be used to scan just the VeeamFLR path that contains the published backups.



Once the VeeamFLR path is selected with the ESET tool, the 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:



The other tool I want to highlight as a possible detection technique when using the data integration API is Total Commander. This tool is a staple for many IT administrators 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 the encryption search may not show files that are encrypted from a threat. The possibility of Veeam Data Integration API in coordination with some of the preferred toolkits in each IT organization's area of expertise are 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 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: http://vee.am/vdapi

Veeam DataLabs: Veeam DataLabs can be used to help you become resilient against ransomware by being a detection as well as a remediation technique. The SureBackup job will run a Veeam DataLab to perform many tasks:

- Ensure recoverability of a backed-up system
- Perform a test on a system like updates, changes to an application, etc.
- Staged and 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 in which a system will not boot or 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.

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 them existing, being encrypted or possibly extracting selected data.

Veeam encryption of backup data

In the war against ransomware, it may seem counter-intuitive to recommend encrypting Veeam backups. This however is the *good* type of encryption; It's encryption as a recommendation for additional resiliency against ransomware and insider threats.

The recommendation here is that you use Veeam encryption on backups wherever possible, including in the first backup. The first backup is usually taken on the same site, close to the source data and is generally on an on-premises backup repository. Additional instances of Veeam backup data, such as through a backup copy job or processing onto the Veeam Cloud Tier should also be encrypted.

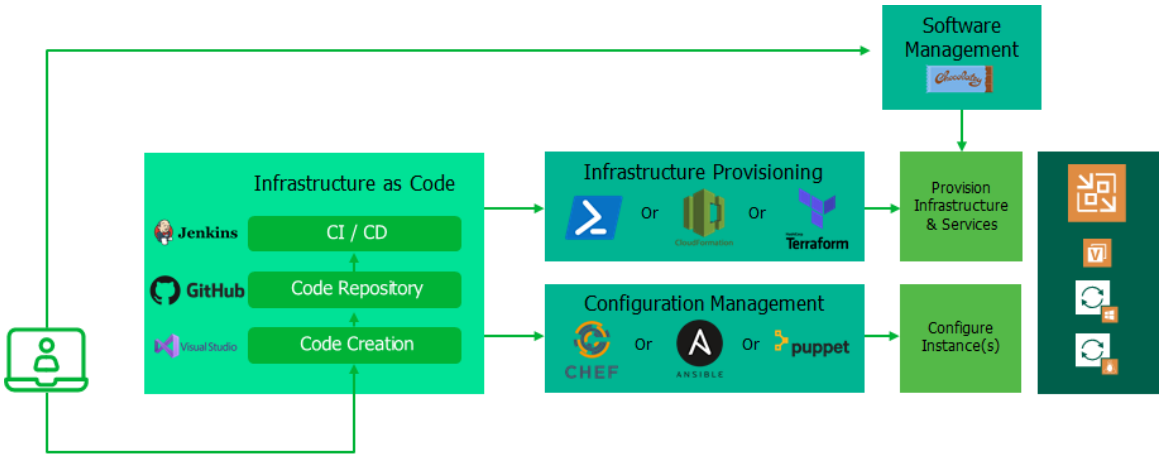
By having the first backup and all subsequent copies of the backup data encrypted, the Veeam backup files are protected against an emerging type of ransomware. There are threat actors that charge ransom to prevent data leaks versus just to decrypt data. The ransom is taking down data that has leaked out of the organization. We would not want a public link with some backup files containing confidential data going out to the highest bidder. Ideally, previous recommendations in this document would prohibit that from happening, but this is an additional protection. Veeam encryption is supported for a backup job, a backup copy job, a backup to tape job, VeeamZIP and tape encryption.

Note: Veeam encryption is not recommended if the repository performs native encryption or supports a secure mode (such as appliances).

Investments in automation

One area that is advisable to have as an additional weapon for ransomware resiliency is in automation. This will specifically help in potential remediation situations, as the original infrastructure may be untrusted. There are many Infrastructure-as-Code techniques available with Veeam, Microsoft, VMware and related technologies.

The various tools in place can provision infrastructure, configuration and key services.



The potential to create a completely new platform in which to restore via automation is a compelling part of a potential recovery scenario. This would be a platform in which you need a new "platform" to restore to but have good Veeam backup data. Consider some of these toolkits as opportunities to rapidly deploy in the event of a need for a complete recovery scenario. Here are a few key pieces of additional content to get acquainted with these technologies:

Veeam VMworld 2018 session:
https://videos.vmworld.com/global/2018/videoplayer/26243

Veeam deployments in Chef (Part 1):
https://vzilla.co.uk/vzilla-blog/cooking-up-some-veeam-deployment-with-chef-automation-part-1

Veeam deployments in Chef (Part 2):
https://vzilla.co.uk/vzilla-blog/cooking-up-some-veeam-deployment-with-chef-automation-part-2

Infrastructure-as-Code example tools:
https://vzilla.co.uk/vzilla-blog/summerproject-infrastructure-as-code-example-tools

Windows operations and using Chocolatey for Windows package management with Veeam Agents:
https://vzilla.co.uk/vzilla-blog/windowsoperationsusingchocolateyforveeamdeployment

Remediation

Despite all of the education and implementation techniques that are employed to be resilient against ransomware, organizations should be prepared to remediate a threat if introduced. At Veeam we have agreed upon the approach to remediating ransomware as:

- Do not pay the ransom
- The only option is to restore data

With the recommendations previously outlined in this document, organizations should be prepared to have layers of resiliency to defend against a ransomware incident. What organizations may not have thought about is specifically what to do when a threat is discovered.

Here are few recommendations for remediation that should be at your disposal should a ransomware incident happen:

Veeam Support: There is a special group within the Veeam support organization that has specific operations to guide customers through data restores in ransomware incidents. You do not want to put your backups at risk; they are critical to your ability to recover.

Communications first: In disasters of any type, 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 mechanisms but expanded for an entire IT operations groups.

Experts: Have a list of security, incident response, identity management, etc. experts that are ready to be contacted if needed. They can be within the organization or external experts. If a Veeam service provider is used, there are additional value adds to their base offering that can be considered (such as Veeam Cloud Connect Insider Protection).

Chain of decision: One of the hardest parts of recovering from a disaster is decision authority. Who makes the call to restore, to fail over, etc.? Have business discussions about this beforehand.

Ready to restore: When the conditions are right to restore, implement additional safety checks before putting systems on the network again. Part of those tips are explained earlier in this document but additional steps can include restoring with network access disabled for a final check.

Restore options: Depending on the situation, maybe a whole VM recovery is best. Possibly a file-level recovery makes sense. Familiarity with your recovery options will help greatly.

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 an additional tool to ensure a threat is not reintroduced.

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

Conclusion: Prepare now, or else!

The threat is real, and the opportunity to prepare is upon us. What are the steps needed to be resilient against ransomware? This paper has outlined several tips around education, implementation and remediation. With the right preparation, the steps here can increase your resiliency against a ransomware incident to avoid data loss, financial loss, business reputation damage and more.

You can find more information about Veeam ransomware resiliency resources at:
http://vee.am/ransomwareseriespapers

About the Author

Rick Vanover (Cisco Champion, vExpert) is the senior director of product strategy at Veeam Software. Rick's IT experience includes system administration and IT management, with virtualization being the central theme of his career recently. Follow Rick on Twitter @RickVanover or @Veeam.

About Veeam Software

Veeam® is the leader in Backup solutions that deliver Cloud Data Management™.Veeam provides a single platform for modernizing backup, accelerating hybrid cloud and securing your data.With 365,000+ customers worldwide, including 81% of the Fortune 500 and 66% of the Global 2,000, Veeam customer-satisfaction scores are the highest in the industry at 3.5x the average.Veeam's global ecosystem includes 70,000+ partners, including HPE, NetApp, Cisco and Lenovo as exclusive resellers.Headquartered in Baar, Switzerland, Veeam has offices in more than 30 countries.To learn more, visit https://www.veeam.com or follow Veeam on Twitter @veeam

VEEAM

Cloud Data

Backup for what's next

5 Stages of Cloud Data Management — start your journey today!

Learn more: veeam.com