Petri IT Knowledgebase Resource
A BWW Media Group Brand

Tips, Tricks and Best Practices for Physical Server & Endpoint Backup

Sponsored by

VEEAM

Tips, Tricks and Best Practices for Physical Server & Endpoint Backup

Presenter: Rick Vanover, Director of Technical Product Marketing & Evangelism for Veeam Software

Moderator: Brad Sams, Petri IT Knowledgebase, Executive Editor at Petri.com

Overview

Organizations have data in many different places that need to be made available. Whether it is a physical server or a desktop, roaming laptop or a few other configurations – that data needs to be protected against everyday occurrences such as lapses in connectivity, hardware failures, file corruption — or even ransomware or theft.

Context

Today, organizations should not struggle with getting data off-site or protecting endpoints. In this webinar, Rick Vanover showcases how the Veeam Agents for Windows and Linux can help organizations keep physical data available.

In the webinar, Rick explained what capabilities exist today for physical server and endpoint backup, off-site data backup and restore options, and where to use different backup strategies.

Key Takeaways

Data in Small Places: Endpoints

One of the more challenging aspects of data protection are endpoints (PCs, laptops, Windows tablets, etc.) that have a seamless integrated experience with corporate IT but may be mobile and/or always off-site.

With 5G coming online in the near future, data being created at the edge, and an increasing number of devices accessing your network from outside the corporate firewall, your exposure to external risks is only increasing.

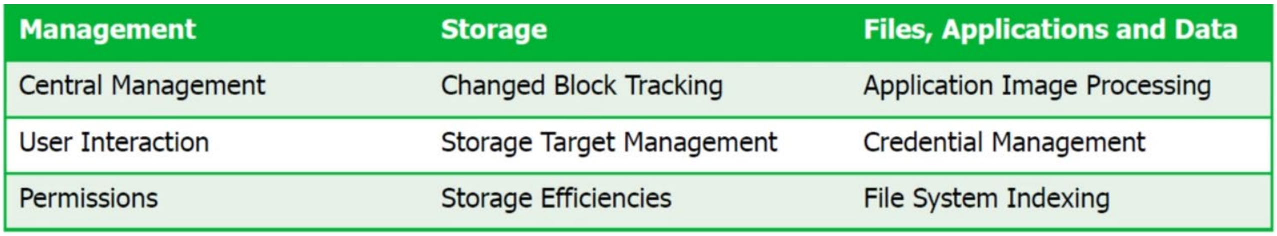
As a practicing IT Pro, it's important to keep in mind that employees are going to do what works for them, not always what is in the best interest of corporate data retention and security.

What Capabilities Exist: Backups

When it comes to backups, Rick discusses three areas of focus: management, storage, and files/applications data.

Central management is very important and Rick encourages organizations to focus on doing this by type or account device type, by using tools like Active Directory Objects or Organization Units (OU). One example rick cites is organizing your devices with profiles like desktops or laptops as this helps profile what backup options are available based on the device type.

User interactions and permissions are important to fully understand as they identify which employees can install and modify their own software. Building in logic to force installs of approved applications or policies to not allow removal of critical company backup software is a simple but key way to automatically protect your environment. While this may seem obvious, users with more access have the ability to control and modify when and what data is backed-up and as an administrator, it's important to understand how this plays into your recovery matrix.



Management	Storage	Files, Applications and Data
Central Management	Changed Block Tracking	Application Image Processing
User Interaction	Storage Target Management	Credential Management
Permissions	Storage Efficiencies	File System Indexing

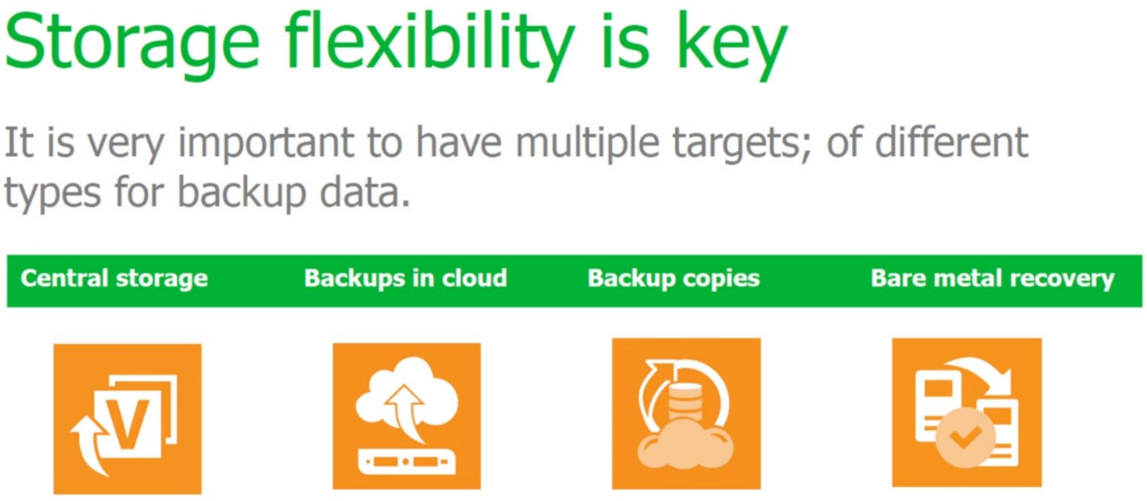
For storage, it is possible to have the ability to Changed Block Tracking for physical server and end-point backup. Veeam built technology to support this granular model for both Linux and Windows but also keep in mind that you need a central management tool to keep tabs on your target devices.

Storage efficiency and the type of backup hardware you are using will be critical to the long-term viability of your recovery operations. You can't simply dump data on to a drive and forget about it, you need to make sure it is properly stored with compression, de-duplication, and using tools like ReFS for increased efficiencies.

When it comes to files, applications, and data, security needs to be maintained. As an example, if the CEO asks for Payroll.xls to be restored, Help Desk staff should be able to restore that file without having the permission to open the document.

What Capabilities Exist: Restore

Much like backups; resources must be dedicated to the restoration of a backup; a backup is useless if you are not able to load it into production. Especially when it comes to older hardware, if you can't get replacement parts for hardware, you need to test that you can run your environment from your backup infrastructure.



Storage flexibility is key

It is very important to have multiple targets; of different types for backup data.

A key test for your backup environment is the ability to move data around. As Rick discusses in the webinar, this is a resiliency technique which comes from storage flexibility.

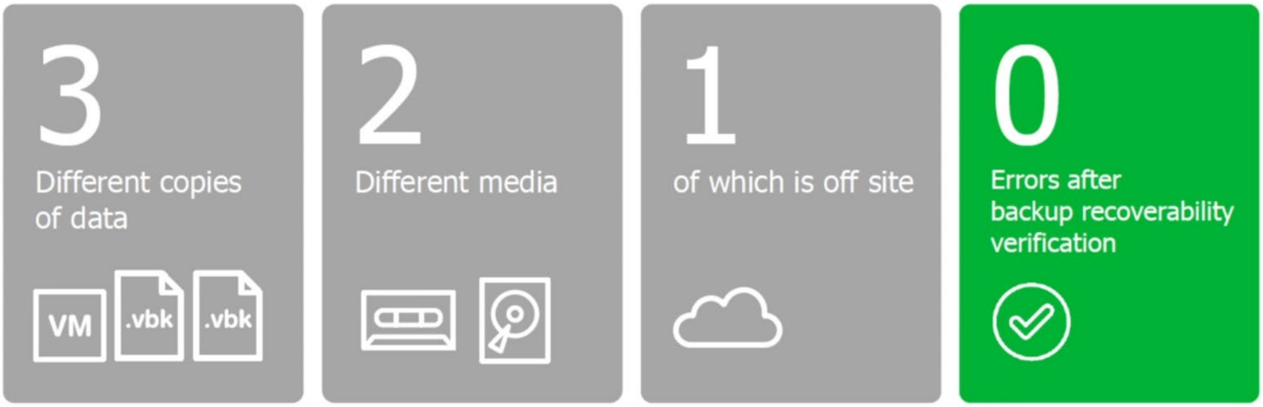
Central storage can be simple things like using tape and the idea of where you physically put your backup machines and hardware. The idea is that your physical copies are organized, safely stored, and easily accessible in the event of a disaster or outage.

While traditional cloud providers like Microsoft and Amazon are good locations for backup storage, there is a large market of service providers who can offer customized solutions that can increase security and reliability of the availability of your backups with minimal overhead to the end user.

But the baseline rule is to have multiple backup copies. The key is to not have a single point of failure from blocking access to your backup copies and the only way you can prevent this is with multiple copies of your data.

3-2-1-0 Rule

Master the 3-2-1-0 Rule



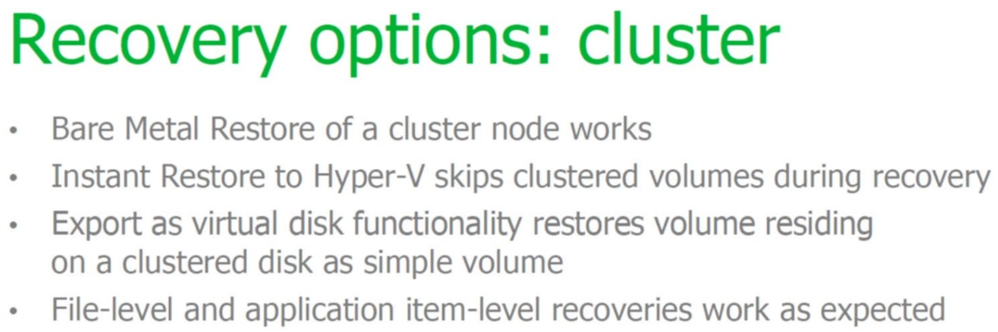
* Don't forget your offline copy!

This basic rule will help you, at minimum, make sure that your data is backed up safely and securely. But it's important to know that just because your data is backed up, doesn't mean that it can be recovered quickly.

Servers and Endpoints:

In the event that you do need to perform a recovery of an application or environment, Veeam's tools provide multiple options for restoring the files or applications. These options include bare metal recovery, exporting as a virtual disk, instant recovery to Hyper-V, application item recovery, restore guest files, and restore to Microsoft Azure.

The key is to be able to restore anything from the entire environment or specific objects inside of a backup file. Meaning, if you can't restore at the file or object level, you have a weakness in your recovery process.



Recovery options: cluster

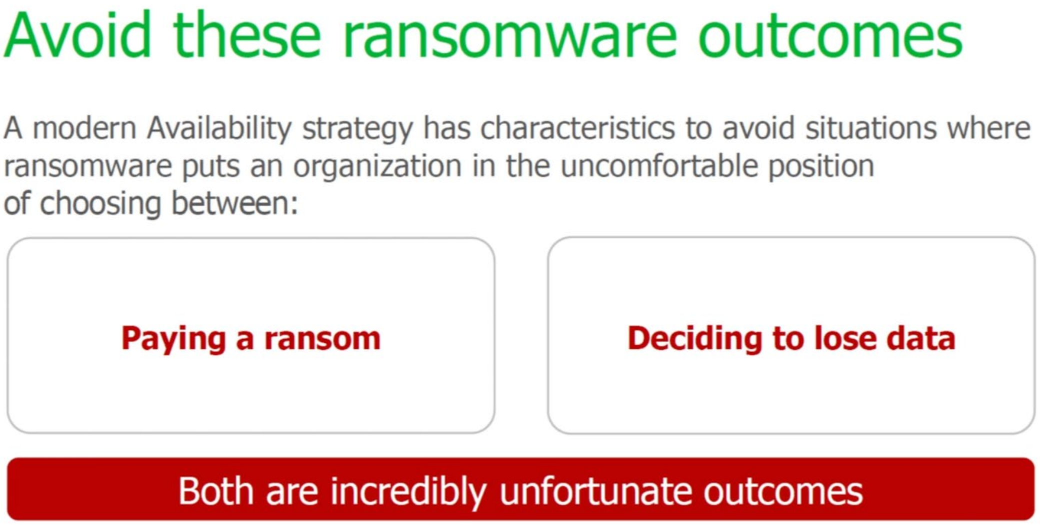
- Bare Metal Restore of a cluster node works
- Instant Restore to Hyper-V skips clustered volumes during recovery
- Export as virtual disk functionality restores volume residing on a clustered disk as simple volume
- File-level and application item-level recoveries work as expected

And for environments with clusters, Veeam has options to restore and service those types of operations too.

Ransomware Tips:

The threat of ransomware continues to grow each year and your best defense is a layered approach. There is also no single magic bullet to defending against these new attacks as they come in many different forms.

The best tip is to educate the end user on what ransomware is and how to avoid it at the user level. This can be accomplished many different ways but having an IT Admin do a seminar on basic virus prevention is your first line of defense.



Avoid these ransomware outcomes

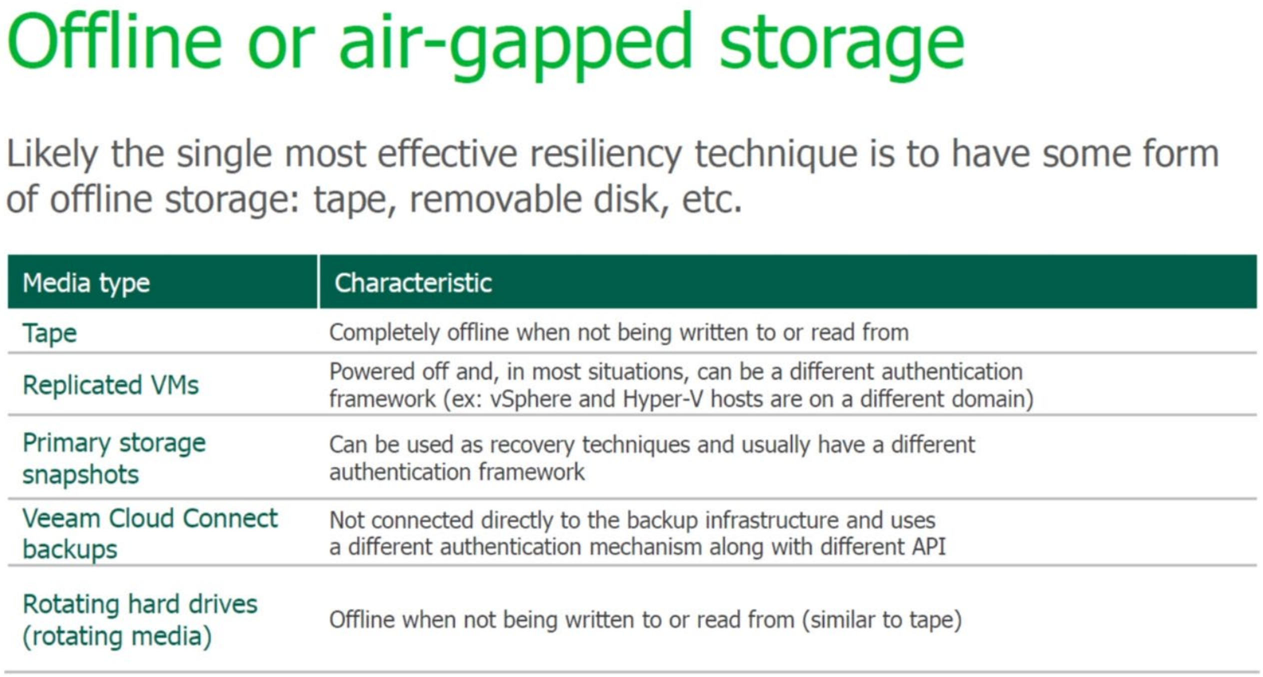
A modern Availability strategy has characteristics to avoid situations where ransomware puts an organization in the uncomfortable position of choosing between:

Paying a ransom

Deciding to lose data

Both are incredibly unfortunate outcomes

Having a resilient backup process in places is critical otherwise, when attacked by ransomware, your options are to either pay the ransom or decide to lose data; both of this outcomes are a net loss for the organization.



Offline or air-gapped storage

Likely the single most effective resiliency technique is to have some form of offline storage: tape, removable disk, etc.

Media type	Characteristic
Tape	Completely offline when not being written to or read from
Replicated VMs	Powered off and, in most situations, can be a different authentication framework (ex: vSphere and Hyper-V hosts are on a different domain)
Primary storage snapshots	Can be used as recovery techniques and usually have a different authentication framework
Veeam Cloud Connect backups	Not connected directly to the backup infrastructure and uses a different authentication mechanism along with different API
Rotating hard drives (rotating media)	Offline when not being written to or read from (similar to tape)

The best technique for avoiding a ransomware issue is to have an air-gapped backup solution. This means that there is no connection between production and the backup storage so that if ransomware does hit your environment, there is no physical connection to the backup media.

Veeam Availability Suite delivers Availability for ALL workloads — virtual, physical and cloud — from a single management console. Veeam helps organizations meet today's service-level and data center Availability objectives for the growing enterprise. Veeam Availability Suite is the premier solution providing the superior data protection capabilities of Veeam Backup & Replication™ paired with the advanced monitoring and reporting of Veeam ONE for holistic coverage of all workloads.