 KNOWLEDGE BASE

# HostedBizz RansomProtect

HostedBizz RansomProtect ensures that your backup data is fully protected. Some customers may have concerns that backup files may be deleted accidentally or maliciously. RansomProtect ensures threats from inside your network are mitigated as well.

## Use Cases

HostedBizz RansomProtect enables you to recover a backup chain deleted by mistake but more importantly it protects you from malicious attacks from outside threats. Backing up your data locally and offsite is no longer a catch all solution as recent attacks show that backup files are being targeted and destroyed. Attackers are aware of retention policies for you backups as well. Instead of simply deleting your backup files, they may choose to corrupt your production data and continually run a backup job to a cloud target. This ages out any useful recovery points you may have and replaces them with backups of already corrupted data.

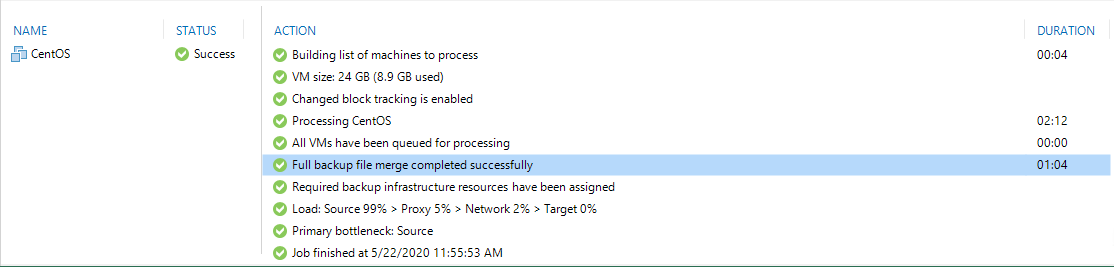
With HostedBizz RansomProtect, backup files deleted accidentally or maliciously are retained in a separate directory. This folder is not visible to the customer or public routing. Backup files that are deleted will remain in this isolated folder for a set amount of days and can be saved and transferred back to a customer once ready to restore data. When using GFS retention settings in a backup copy job, you can also restore from the archival backups if an attacker deletes or "ages out" the offsite chain. With HostedBizz RansomProtect, you can ensure that even a devastating attack is recoverable.

## How It Works

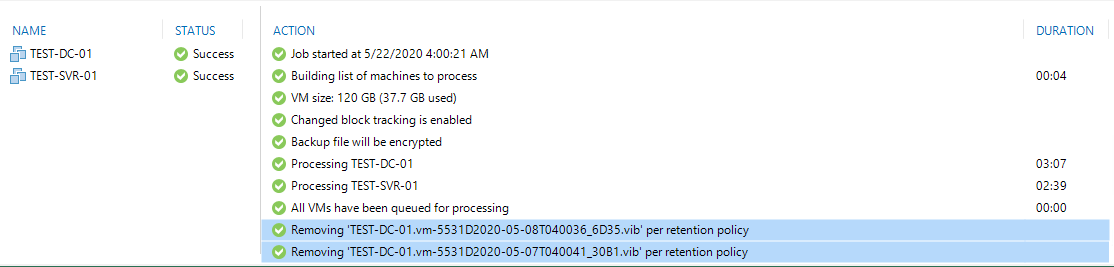
Your Veeam Cloud Connect account has RansomProtect enabled by default to store deleted files for 5 days, if you would like this increase please contact your HostedBizz Account Manager. You do not need to make any changes to the job or your Veeam configuration. However, on the service provider side, aged out or deleted backups will be moved to a Recycle Bin directory. The storage used in this Recycle Bin does not consume any space from your Cloud Repository.

For example, in the screenshots below you can see the run history of two different Offsite Backup Jobs. Depending how the job is configured changes how it’s displayed, but either the old points are deleted as per the retention policy or they are merged into the full at the start of the chain. Note that if the latter, you do not see the increments being deleted in the job statistics, but they are deleted after the merge.

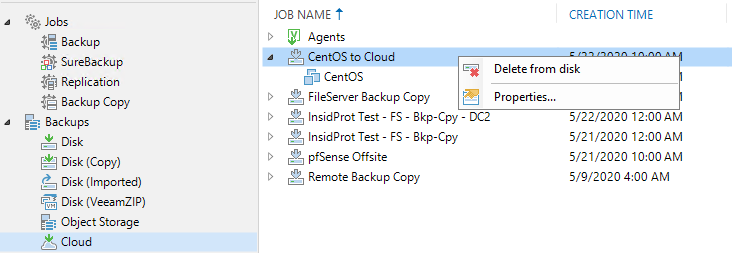
This is the example with the merge, you don’t see the increments being deleted, but they are moved to the recycle bin after the merge:



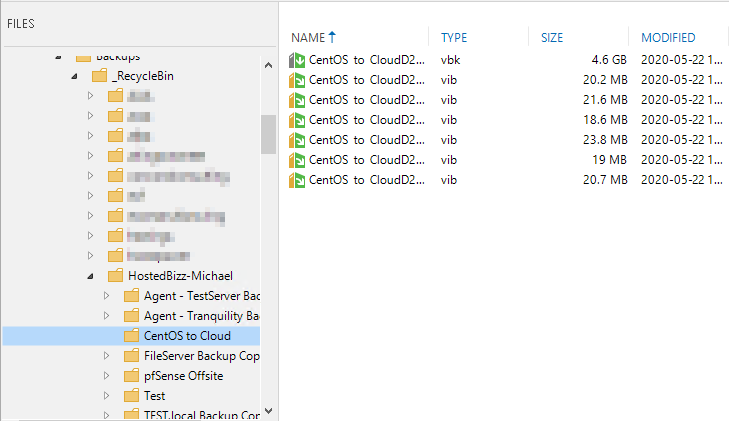
This is the example with the deleted points, since the retention policy was met (the job had synthetic full backups enabled) it deletes the obsolete part of the chain entirely:



Beyond saving aged out backup files, RansomProtect will also hold on to servers that have been deleted as well. To demonstrate, we can delete the entire backup chain of the Offsite Backup job from the local Veeam console.



Once deleted, you will again not be able to view or restore data from this backup chain. However, with assistance from HostedBizz, you will be able restore the backup files with RansomProtect. Back on the service provider console, we can see all restore points that were removed for this job. These files can then be transferred back to the tenant Veeam server for restoration.



## Limitations

**Veeam full backup files (.vbk) and Veeam metadata files (.vbm) are the only two files that can be imported into Veeam and restored from**.

It’s important to note the above as in a situation where you must leverage RansomProtect to recover your backups, only the .vbk will be usable as RansomProtect does **not** preserve the .vbm of the chain. Because the .vbm is not present all .vib files are equally non-usable.

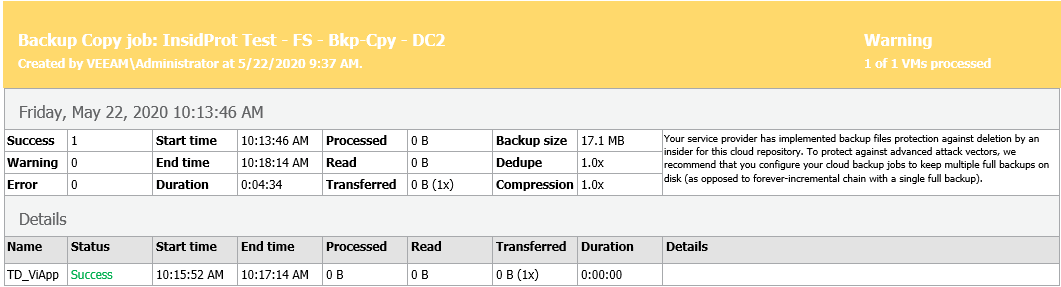
This means in that with jobs that utilize Forever Forward Incrementals, only the oldest point, the .vbk will be useful for a restore. Forever Forward can be configured on Backup Jobs and also is the only mode that a Backup Copy works in.

Jobs that utilize periodic synthetic or active full backups (Forward Incremental) will also be limited to their oldest .vbk, but this is likely not going to be the oldest point in the chain. Jobs that use Reverse Incremental Backup will always have the .vbk as the newest point.

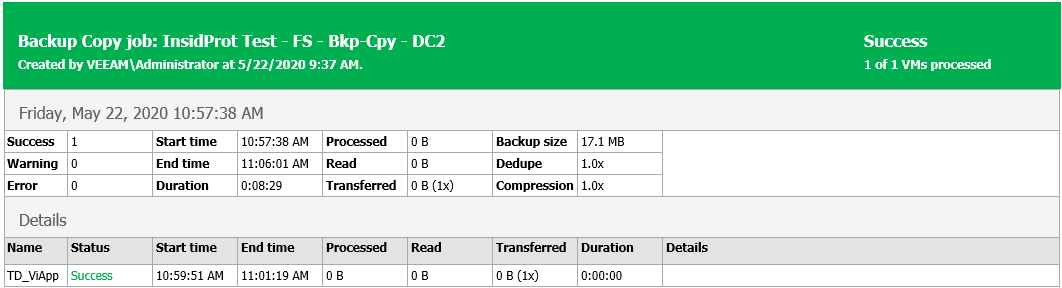
You can mitigate the concerns of Forever Forward and Forward Incrementals by using the GFS points on Backup Copy jobs to get a weekly full backup that is independent of the chain. Starting in Veeam 10 this feature is also available on Backup Jobs.

The GFS archiving is recommended when using RansomProtect, and it is recommended that with a Backup Copy job that you use at least 1 Weekly archival backup. These backups exist outside of the Backup Copy job chain and are stored as .vbk files. Meaning that they are able to be imported and have data restored in your Veeam infrastructure. Not using Veeam GFS backups with your Backup Copy job will result in a warning every time it runs.

See below for a screenshot of this warning:



Note that even though the backup itself is successful there is a warning. Once you enable at least one GFS point on the Backup Copy the warning is cleared:



Alternatively, you can make a RegEdit to clear the warnings as well, just understand before doing so that the RansomProtectand GFS recommendations exist for a reason.

Veeam KB: <https://www.veeam.com/kb2439>