VEEAMON 2023

Veeam Backup: Secure Restore at scale

Ton Huynh

Principle Systems Engineer

Veeam Software

Johan Huttenga

Staff Solutions Architect

Veeam Software

About Ton

Principal Systems Engineer at Veeam®

A background in enterprise solutions design, architecture and integration involving both on-premises and cloud technology stacks.

In my free time you can find me at Disneyland with my family or watching my kids play sports.

About Johan

Staff Solutions Architect at Veeam

A background in operations, solutions architecture, automation, development and cloud and is responsible for joint Microsoft and Microsoft Azure technical initiatives.

In my free time, you can find me coding, hiking, paddle boarding or building something out of Legos with my three-year-old.

Agenda

- Ransomware is a key reason for backup
- As a customer I want to ensure that my backup data is clean
- How can perform data security scanning and integrate this with monitoring or a SIEM solution at scale in the real world?

We'll be discussing a real customer scenario, with real code and a real demo

VEEAMON 2023

The use case for "Secure Restore" at scale

Customer profile

Environment

3100 VMs

(Windows and Linux)

150

Veeam Agents

500 TB

NAS Backup

Veeam Backup and Replication™ v11a

Veeam ONE™ v11a

10 proxy servers:

- Virtual
- Physical

Seven Scale-Out Backup Repositories™:

- Mix of two to six extents

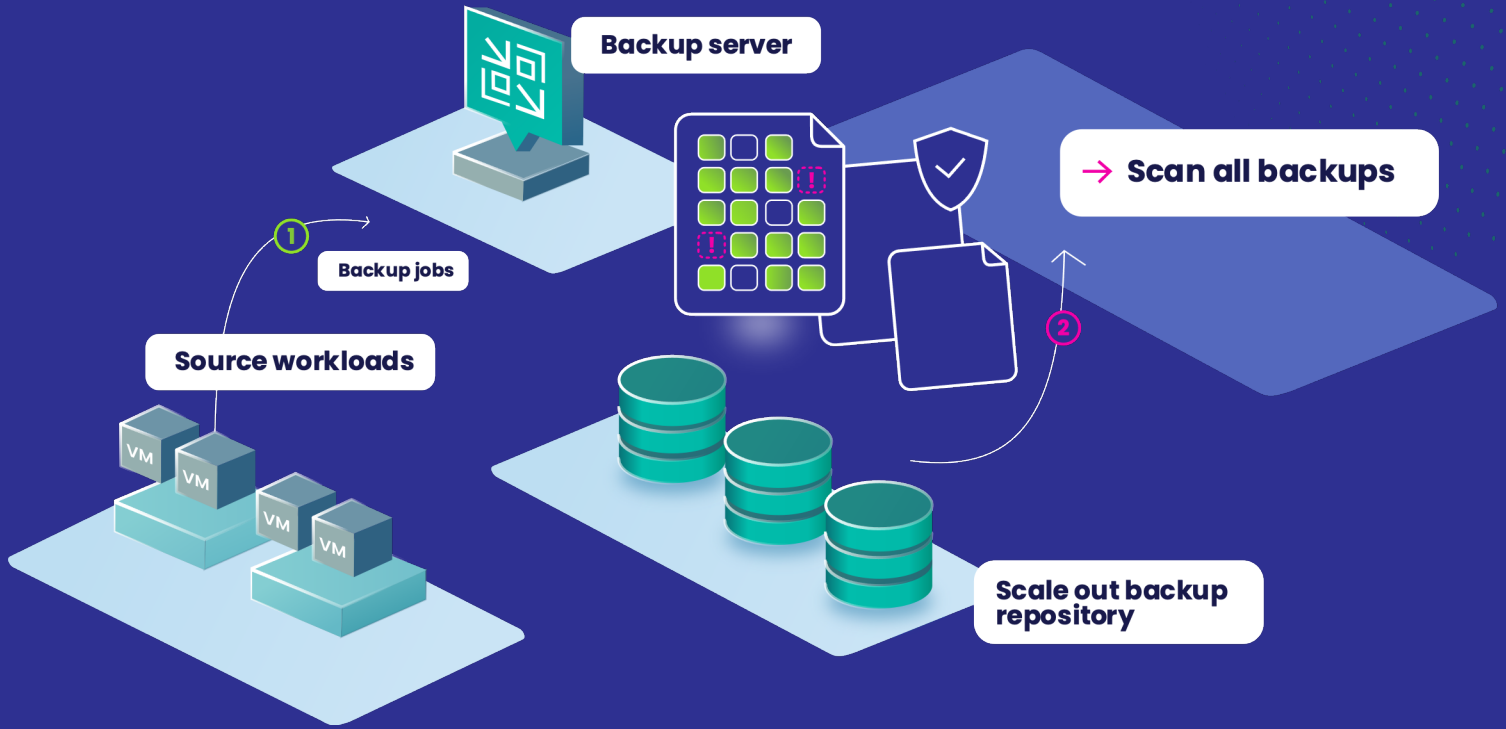
Five standalone repositories

Linux hardened repositories

S3 object storage

Tape

Customer request



VEEAMON 2023

Secure Restore vs. data integration API

Secure Restore

Helps prevent malware and other security threats from compromising backups

Scans backup files for malware and other security threats before allowing them to be used in production

Verifies files are clean and safe before recovery into production

Helps protect against the risk of data loss due to security threats

Secure Restore with SureBackup®

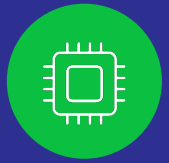
Allows testing and validation of backups and replicas without affecting production

Creates an isolated environment for testing

Runs security and compliance scans in the isolated environment

Helps identify and mitigate security risks before they impact production

Helps ensure compliance with data protection regulations and industry standards



Can be used for testing patches, upgrades and other changes before deploying them in production

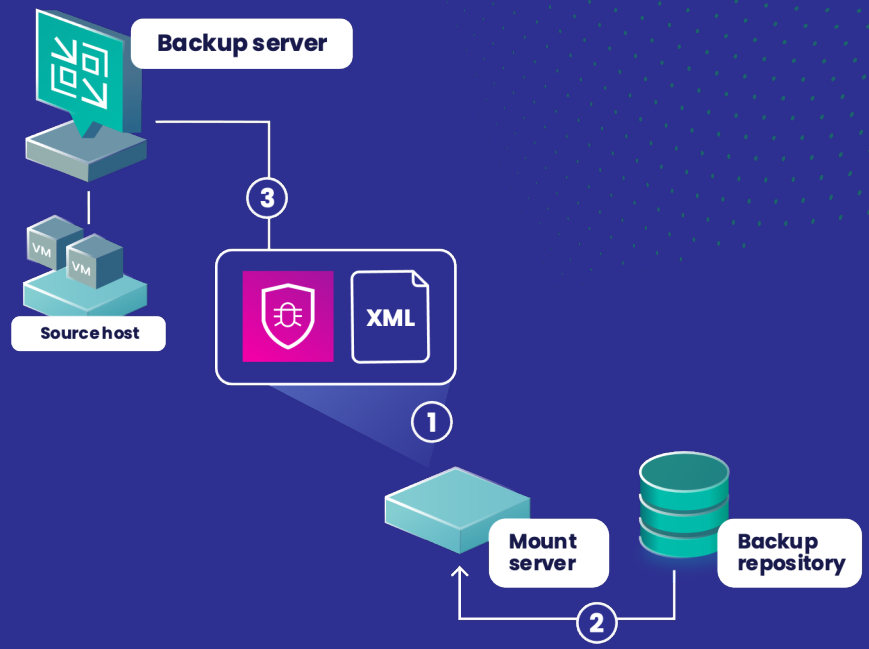
Secure Restore considerations

You can perform secure restore only for machines that run Microsoft Windows.

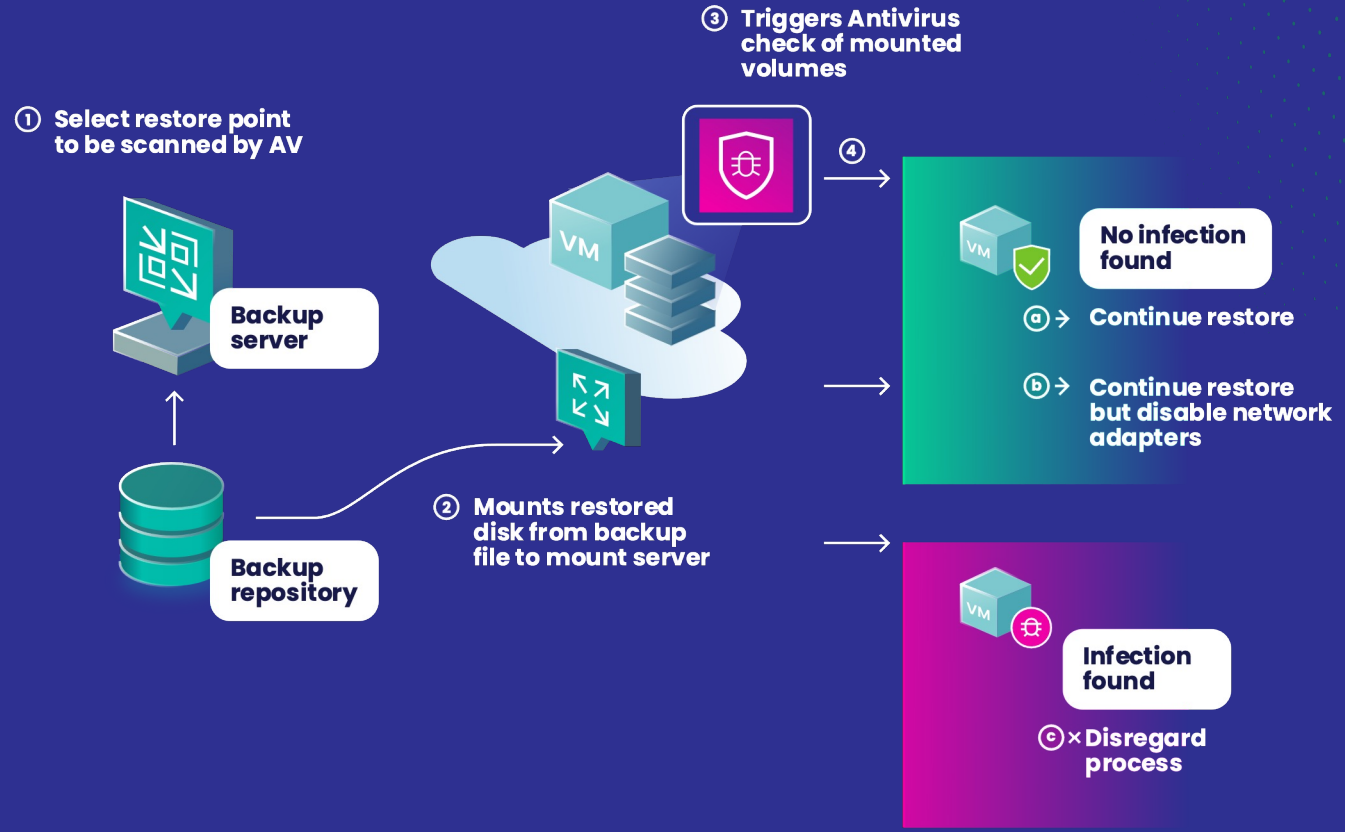
The antivirus software must be installed on the mount server and support the command line interface (CLI).

Predefined antivirus software

- Symantec protection engine
- ESET
- Windows Defender
- Kaspersky security 10 and 11
- Bitdefender endpoint security tools



Secure Restore process



Where is Secure Restore enabled

- Instant Recovery
- Entire VM restore
- Virtual disks restore
- Restore to Microsoft Azure
- Restore to Amazon EC2
- Restore to Google compute engine
- Disk export
- SureBackup

Veeam data integration API

Mount backed-up data via either iSCSI on Windows or FUSE on Linux:

VM backups

VM replicas

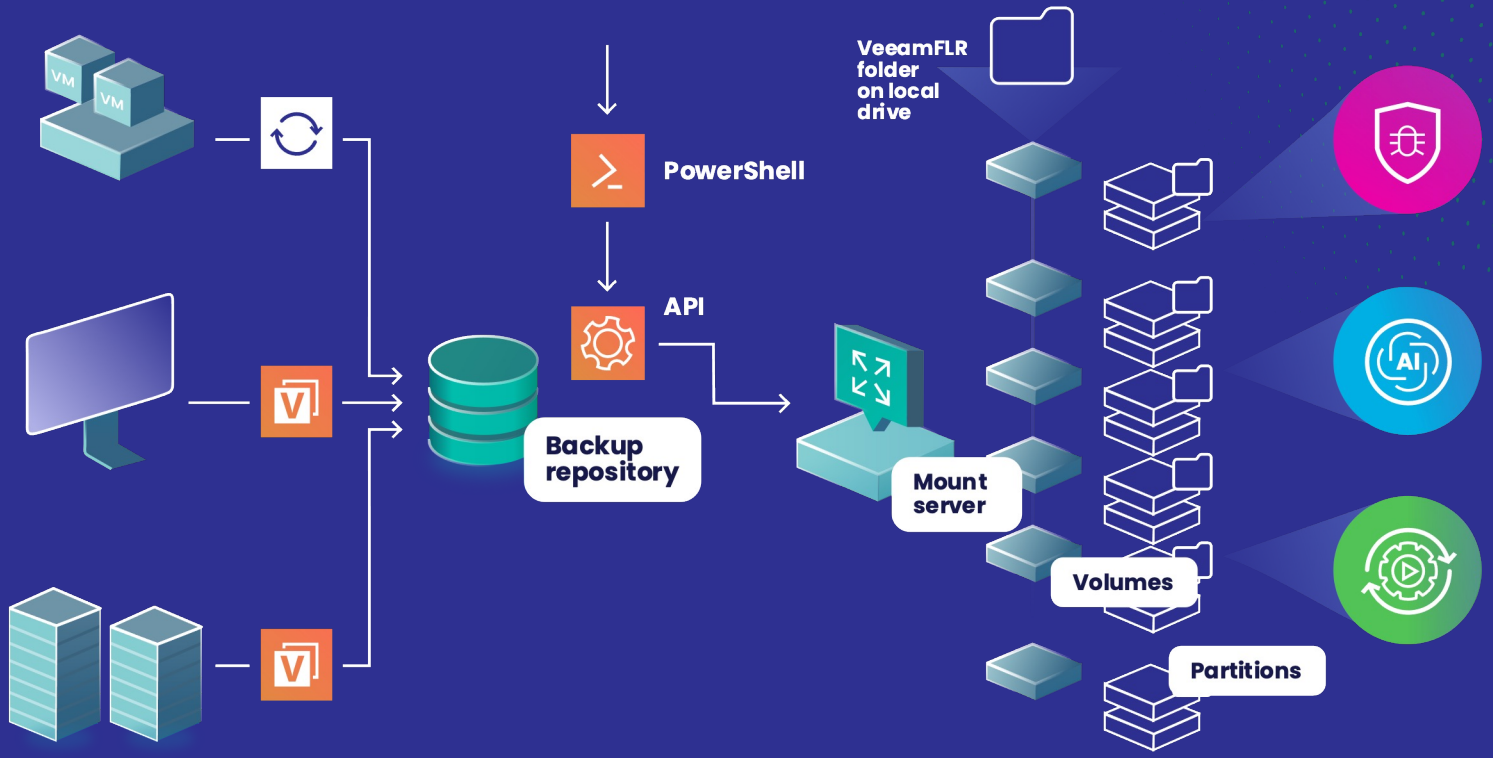
Computer backups

Operation	Cmdlet
Mounts the content of backup files using the iSCSI protocol	Publish-VBRBackupContent
Returns sessions that are running to mount the backup content to iSCSI target servers	Get-VBRPublishedBackupContentSession
Returns details on the mounted content of backup files	Get-VBRPublishedBackupContentInfo
Unmounts content of backup files from iSCSI target servers	Unpublish-VBRBackupContent

VEEAMON 2023

Building on data integration API at scale

Veeam data integration API



Data integration API PowerShell

Get restore point

```
$RestorePoint = Get-VBRRestorePoint -Backup $(Get-VBRBackup -Name $JobName) -Name $MachineName |
Sort-Object -Property CreationTime | Select -Last 1
```

Publish via iSCSI

```
Publish-VBRBackupContent -RestorePoint $RestorePoint -AllowedIPs "x.x.x.x" –RunAsync
```

Publish automatically

```
$Credential = Add-VBRCredentials -User "server\Administrator" -Password "Pa$$w0rd"
Publish-VBRBackupContent -RestorePoint $RestorePoint -TargetServerName "server"
-TargetServerCredentials $Credential
```

Publish via Fuse

```
$Credential = Get-VBRCredentials -Name "linuxadmin"
Publish-VBRBackupContent -RestorePoint $RestorePoint -TargetServerName 192.0.1.100
-TargetServerCredentials $Credential -EnableFUSEProtocol
```

PowerShell integration with Defender

Import libraries

```
Import-Module -Name Defender.psd1
Import-Module -Name Veeam.Backup.PowerShell
Import-module -name "C:\Program Files\Veeam\Backup and
Replication\Console\Veeam.Backup.PowerShell\Veeam.Backup.PowerShell.psd1"
```

Get restore point

```
$DefenderLatest = Get-Childitem 'C:\ProgramData\Microsoft\Windows Defender\Platform’ |
? { $_.PSIsContainer } | sort CreationTime -desc | select -f 1
$DefenderProg = "C:\ProgramData\Microsoft\Windows Defender\Platform\$DefenderLatest\MpCmdRun.exe"
```

How it works

Get **BR-DataIntegrationAPIAtScale** from
https://github.com/VeeamHub/powershell

- Orchestrates tasks per node
- Mounts content of backup files
- Starts AV scanning process
- Handles logging and reporting
- Aggregates results

Scaling and best practices

Mounting and scanning is easy, orchestrating and scaling is harder

- Use all available Windows or Linux servers
- Some PowerShell command-lets are slow, for example, you can optimize and or cache operations that retrieve Veeam restore point information
- One scan per 'mount server', once a scan is finished, setup the next mount
- Results are the most important part, aggregate via centralized logging, a database or a solution of your choice (maybe a SIEM like Azure Sentinel)
- Scanning through mount points takes CPU and RAM from the AV product
- Generate a pretty report afterwards

VEEAMON 2023

Demo


Thank you!
VEEAMON2023