

How Ryanair Achieved Operational Resiliency Through Fortified Backups



Paul Walsh

Senior Systems Engineer
Ryanair



Rasmus Haslund

Principal Technologist
Veeam Software



210

'Gamechangers'
on order
197 seats



409

B737-Next Gen
189 seats



29

Airbus A320s
180 seats



505

aircraft for summer 2022



What do I do at Ryanair?



Part of IT team
under CTO

- 500 people in IT.
- 72 people in support.



Responsibility

- All ESXi/Hyper-V hosts.
- All storage systems (Dell EMC Powerstore).
- Backups/archiving of all Ryanair back-office systems.



Challenges
in my role

- Growing data volumes.
- Need to manage all this within a reasonable budget.

Historical layout





Backups are target #1

What is an immutable backup?



Preventing deletion of blocks of data or associated metadata until the expiration date set is met

A compliant hardened repository

SEC 17a-4(f), FINRA 4511(c)
and CFTC 1.31(c)-(d)

Cohasset Associates

SEC 17a-4(f), FINRA 4511(c) and CFTC 1.31(c)-(d)
Compliance Assessment
Veeam Backup & Replication

Abstract

SECURE TRADING COHASSET'S INSIGHT

Cohasset's practice is the delivery of securities industry compliance services, including governance professional consulting services, to regulated entities and their regulated organizations, including those in the financial services industry. Cohasset serves both domestic and international clients, aligning information technology, compliance, risk management, and business processes and facilitating regulatory compliance and oversight while generating measurable business outcomes.

Cohasset has assessed the spectrum of storage and backup technologies available to meet the requirements of the Securities and Exchange Commission (SEC) Rule 17a-4(f), as defined by 1) the No Action Letter in 1993 allowing broker dealers to use non-redundant electronic records under Rule 17a-4(f) and 2) the issuance of Rule 17a-4(f) and 31(e) of the Securities Exchange Act of 2003, which authorizes the use of reliable electronic records, subject to certain record keeping costs, to prevent premature deletion requests.

It is Cohasset's opinion that Veeam Backup & Replication, version 11.0, when properly configured, meets all five requirements related to the recording and retention of electronic records in SEC Rule 17a-4(f) and FINRA Rule 4511(c). Additionally, the baseline capabilities of Veeam Backup & Replication meet the principles-based requirements of CFTC Rule 1.31(c)-(d).

12800 Whitehaven Drive, Suite 100 | Minneapolis, MN 55440-6547 (USA) | +1 952 327 1550 | www.cohasset.com

February 2021



https://www.veeam.com/compliance-assessment-report-cohasset_wpp.pdf

White paper for IT professionals
(Veeam administrators)

veeAM

Protect against Ransomware with Immutable Backups: a Veeam Guide

Including SEC Rule 17a-4(f), FINRA Rule 4511 and CFTC Rule 1.31(c)-(d) compliant configuration

Hannes Kasperick,
Principal Analyst,
Veeam Product Management Team

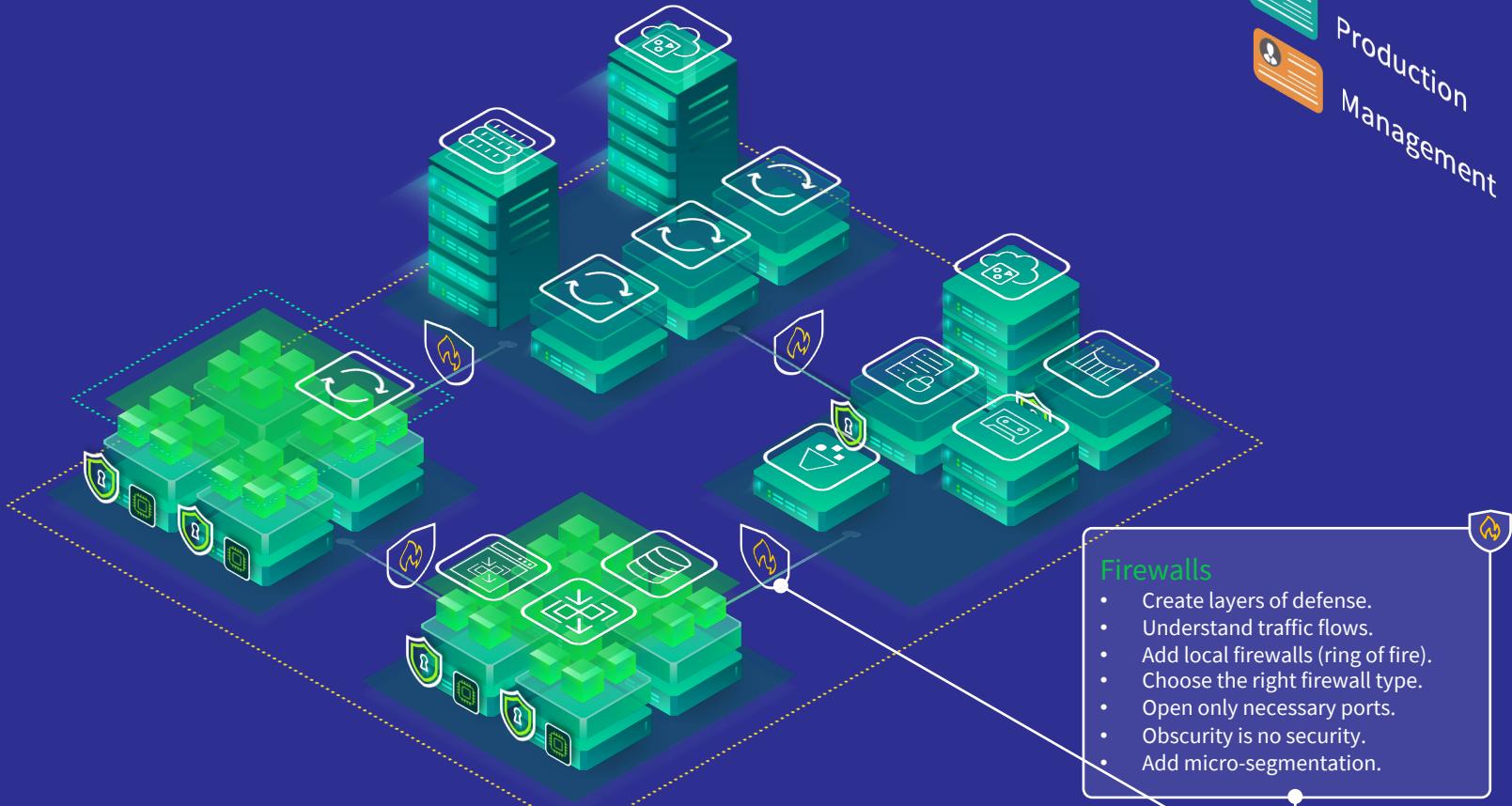


Veeam Backup & Replication v11 F20210309
Date: March 25, 2021



<https://www.veeam.com/wp-guide-protect-ransomware-immutable-backups.html>

Network fortification



Network fortification

Firewalls

- Using NSX intelligence we can understand our network traffic.
- Using NSX segments and Micro segmentation we protect servers.
- Using NSX IDS/IPS we can detect/prevent/alert on suspicious traffic.



The screenshot shows the NSX Intelligence interface under the 'Recommendations' tab. It displays a network graph and a table of recommended policies. The table has columns for Name, Sources, Destinations, Services, Profiles, Applied To, Action, and Default Rule. The 'Rules' tab is selected, showing 9 rules applied to 3 groups. The rules listed are:

Name	Sources	Destinations	Services	Profiles	Applied To	Action	Default Rule
Hello VeeamON	(9)	Applied To: 3 Groups	None	None	None	Allow	None
Rule-1 (VLAN)		HTTP	None			Allow	Allow
Rule-2 (VLAN)		SAP Exchange...	None			Allow	Allow
Rule-3 (VLAN)		MS-DS-TCP	None			Allow	Allow
Rule-4 (VLAN)		Win 2008 - RPC...	None			Allow	Allow

Buttons at the bottom include CANCEL, CONTINUE LATER, and PROCEED.

IDS/IPS & Malware Prevention

Distributed Rules

+ ADD POLICY			+ ADD RULE			CLONE		
	Name	ID						
...	Qualys Bypass	(1)						
...	Zero Day Attacks	(1)						
...	vCenter	(1)						
...	Veeam	(4)						

The screenshot shows the vSphere NSX interface under the 'Networking' tab. The left sidebar includes options like Network Overview, Network Topology, Connectivity, Segments, Network Services, P Management, and Settings. The 'Segments' section is currently selected. The main area displays a table of segments, with the first few rows highlighted in green. Buttons at the bottom include REFRESH and ADD SEGMENT.

Backup server



Segmentation

- Zone: management.
- Network: backup (IPv4 or IPv6).
- Domain: management (Kerberos).
- Firewall: on server (traffic rules).

Secure infrastructure

- TPM 2.0 + Attestation report + alerts.
- Network isolation for IPMI/iDRAC/ILO.
- Principle of least privilege.

Hardware security

- UEFI, secure Boot with TPM+PIN.
- Server locks.
- TPM 2.0.

Physical security

- Role-based access control.
- Locks on equipment racks.
- Biometric access, log & screen people.
- Surveillance > CCTV.

VIRTUAL MACHINE



BIN/LIBRARY

OPERATING SYSTEM



Veeam Backup & Replication Server

1. Move Veeam Console to Management VM.
2. Add user accounts with right role(s) (console).
3. Remove BUILTIN\Administrators Group (console).
4. Activate 2FA per account ([New V13](#)).
5. Enable auto logout ([New V12](#)).
6. Use encryption on all backup jobs.
7. Enable data encryption for configuration backups.
8. Disable remote desktop service.
9. Disable remote registry service.
10. Ensure reliable time source.

VM security

- Disable/remove unnecessary features.
- Use 2FA to access the VBR server.
- Use hardened VM templates (CIS).
- Virtualization based security.

Regular update & patch

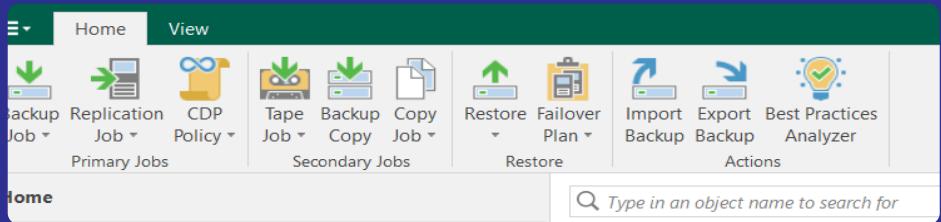
- Hypervisor.
- VM operating system.
- App Veeam Backup & Replication™.

Segmentation

- Zone: management.
- Network: back-end management.
- Domain: management (Kerberos).
- Firewall: on edge (traffic rules).

Veeam Console Best Practices

- Run the inbuilt Veeam Best Practices Analyzer.
- Enable all the Best Practices that are suitable for your environment.
- Limit the number of backup administrators.
- Enable 2FA for backup admins.
- Enable console timeout.



Best Practices Analyzer

The following best practices are guidelines from data protection and security experts. Not following them exposes your Veeam deployment to unnecessary security risks, reduced chances of successful recovery following a cyber attack, affects backup infrastructure reliability etc.

Best Practice	Status
Backup infrastructure security	
Remote Desktop Service (TermService) should be disabled	Passed
Remote Registry service (RemoteRegistry) should be disabled	Passed
Windows Firewall should be enabled	Passed
Product configuration	
MFA for the backup console should be enabled	Passed
Immutable or offline (air gapped) media should be used	Passed
Password loss protection should be enabled	Passed
Configuration backup should be enabled	Passed
Configuration backup should be encrypted	Passed
Backup server should not be a part of the production domain	Passed

Analyze **Suppress**

Reset All **Close**

Copy to Clipboard

Security

User or group: [redacted] assigned Role: Veeam Backup Administrator

Add... Edit... Remove Reset MFA

Require two-factor authentication for interactive logon

Enable auto logoff after 10 min of inactivity

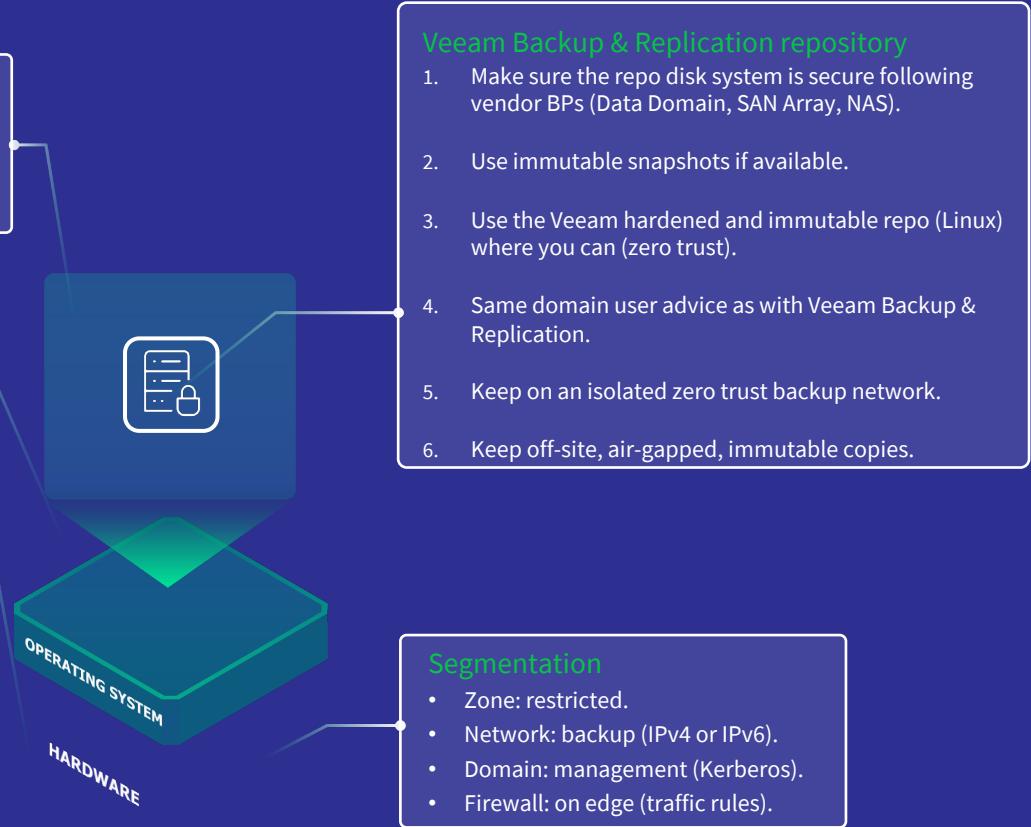
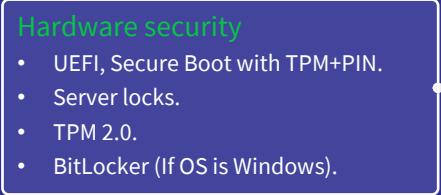
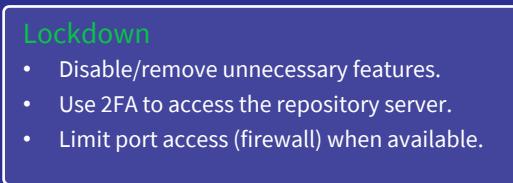
OK Cancel

Veeam
Backup & Replication 12

Enter the code from your authenticator app.

Confirmation code:

Repository server



Repository server monitoring

Use Veeam ONE to monitor repository

- Enable Veeam ONE™ monitoring of Veeam Backup & Replication.
- Enable Veeam ONE alarms for repository changes.

Define Alarms

Selected object: Backup Infrastructure

Type	Name	Assigned to	State
Backup repository connection failure	Backup Infrastructure	Enabled	
Backup repository free space	Backup Infrastructure	Enabled	
Backup repository ReFS data integrity issue	Backup Infrastructure	Enabled	
Backup repository version is out-of-date	Backup Infrastructure	Enabled	
Immutability change tracking	Backup Infrastructure	Enabled	
Immutability state	Backup Infrastructure	Enabled	
Scale-out backup repository data transfer session...	Backup Infrastructure	Enabled	

Summary Monthly Summary Alarms **Protected Data** Tasks & Events

Virtual Machines Computers

Job Status	VM	Latest Restore Point	Restore Points	Job Name	Job Type	Next Job Run
Success		05/04/2023 22:12:55	36		Backup	06/04/2023 22:10:00
Success		05/04/2023 23:07:24	31		Backup	06/04/2023 23:05:00
Success		05/04/2023 17:39:03	34		Backup	06/04/2023 17:33:00
Success		05/04/2023 22:03:58	34		Backup	06/04/2023 22:00:00
Success		05/04/2023 17:52:25	31		Backup	06/04/2023 17:50:00
Success		05/04/2023 17:43:12	29		Backup	06/04/2023 17:40:00
Success		05/04/2023 17:43:12	29		Backup	06/04/2023 17:40:00
Success		05/04/2023 17:43:12	29		Backup	06/04/2023 17:40:00
Success		05/04/2023 17:43:12	29		Backup	06/04/2023 17:40:00
Success		05/04/2023 17:43:12	29		Backup	06/04/2023 17:40:00
Success		05/04/2023 17:43:12	29		Backup	06/04/2023 17:40:00

Summary Monthly Summary Alarms Protected Data

Repository Overview

	0 running tasks	
	Concurrent tasks limit	Not limited
	Repository type	Linux Hardened
	Immutability	28 days
	Stored VMs and computers	65
	Full backups	69.4 TB
	Incremental backups	5.2 TB
	File backups	0 KB
	Short-term file backups	0 KB
	Long-term file backups	0 KB
	Application backups	0 KB

Capacity Planning

	Capacity	106.9 TB
	Free space	85.4 TB
	Out of space	More than 1 year

Backup job/copy job/replica monitoring

Use Veeam ONE to monitor Jobs

- Enable Veeam ONE monitoring of Veeam Backup & Replication.
- Enable Veeam ONE alerts for job status.
- Enable tracking of unusual changes to backups.
- Enable email alerts from Veeam Backup & Replication and Veeam ONE.

The screenshot displays three main sections of the Veeam ONE interface:

- SUMMARY**: Shows Duration (09:10), Processing rate (121 MB/s), and Bottleneck (Target). A green box highlights the Duration value.
- SUMMARY**: Shows Duration (32:50), Processing rate (135 MB/s), and Bottleneck (Target). A green box highlights the Duration value.
- Processing Group: Job**: A log of events with timestamps. A green box highlights the first event: "1 restore point removed by retention policy from VM". The log shows several such events occurring at regular intervals.

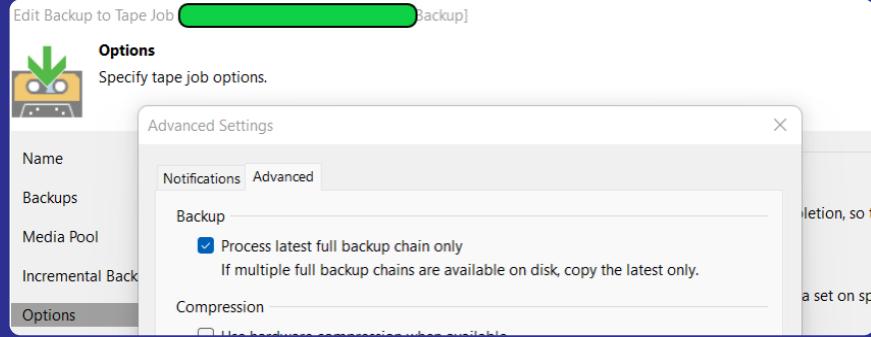
Alarms tab selected in the navigation bar. The Alarms table lists two warnings:

Status	Time	Source	Type	Name
Warning	13:54:39	This object	Unusual job duration	Duration of job "Job Replication" (290.6%) is above the configured threshold (250.0%)
Warning	03:54:41	Job Replication		

Long-term storage of data

Using Veeam TAPE backup and AWS VTL

- Eliminates CRC errors\tape damage.
- Eliminates monthly purchase of tapes.
- Unloading and loading of tape libraries.
- Cleaning drives\library maintenance.
- Shipping tapes off site/retrieving tapes from off site.
- Seamless migration from physical tape to VTL.
- Use synthetic full instead of reverse incremental allows for a longer tape window.

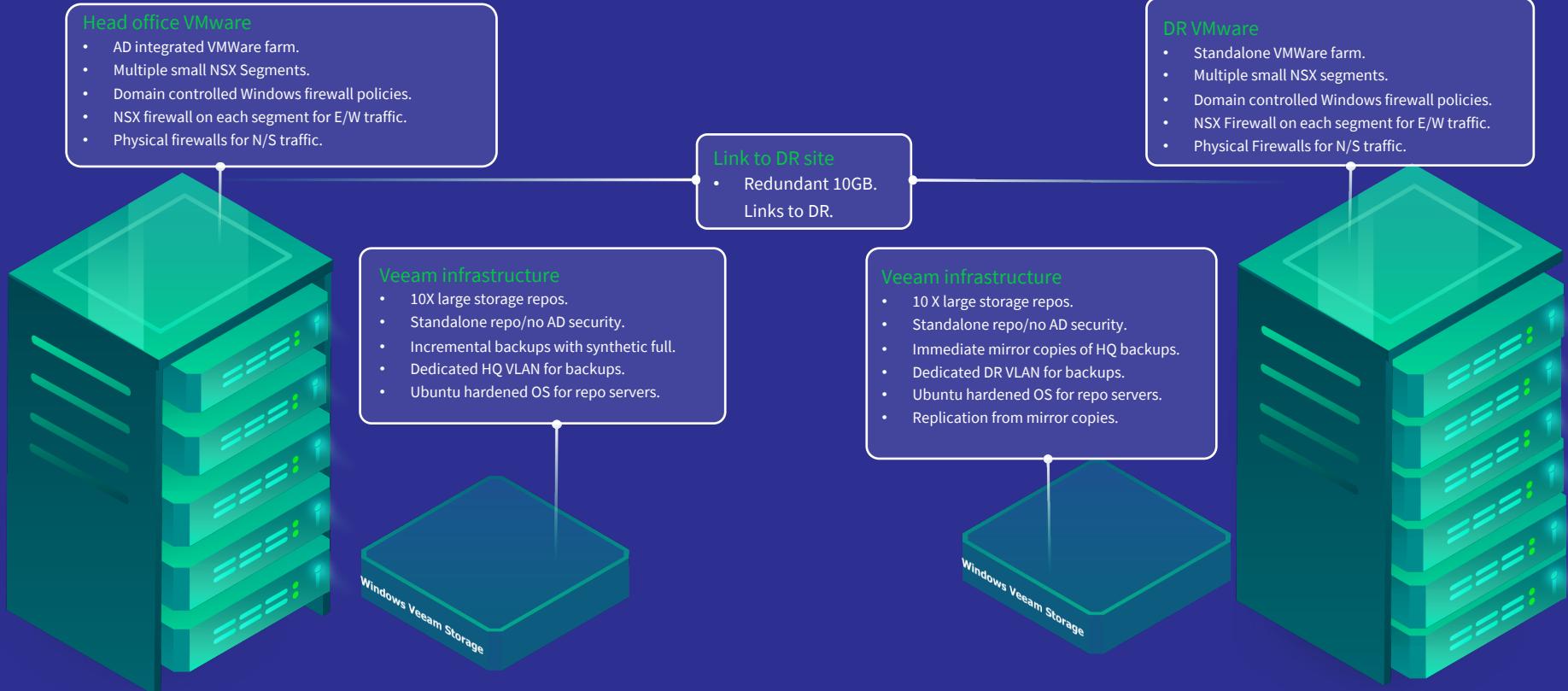


Files:

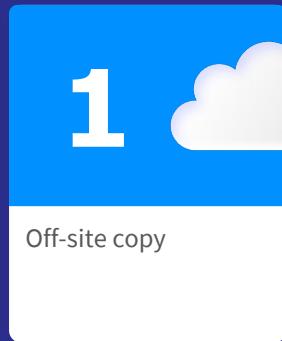
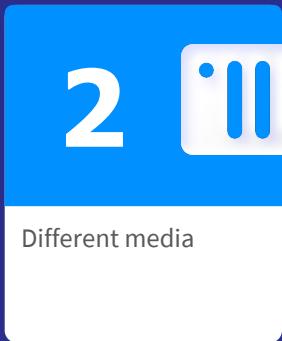
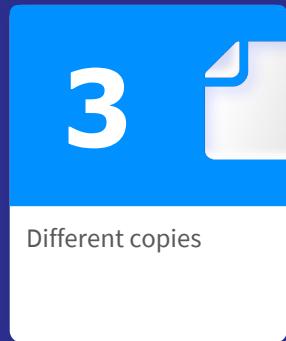
Name	Data Size	Backup Size	Deduplication	Compression	Date	Immutable Until
IMMU - BackupD2023-04-05T224510_32B5.vib	16.7 GB	7.82 GB	1.1 x	2.0 x	05/04/2023 22:45:10	03/05/2023
IMMU - BackupD2023-04-04T224516_0FCA.vib	18.7 GB	8.53 GB	1.2 x	1.9 x	04/04/2023 22:45:16	03/05/2023
IMMU - BackupD2023-04-03T224528_4463.vib	16.9 GB	8.04 GB	1.0 x	2.0 x	03/04/2023 22:45:28	03/05/2023
IMMU - BackupD2023-04-02T224523_04E7.vib	13.5 GB	6.52 GB	1.0 x	2.1 x	02/04/2023 22:45:23	03/05/2023
IMMU - BackupD2023-04-01T224509_F847.vib	9.58 GB	4.14 GB	1.0 x	2.2 x	01/04/2023 22:45:09	03/05/2023
IMMU - BackupD2023-03-31T225632_718D.vbk	2.19 TB	1.49 TB	1.2 x	1.3 x	31/03/2023 22:45:30	03/05/2023
IMMU - BackupD2023-03-30T224528_A729.vib	14.4 GB	7.12 GB	1.1 x	1.9 x	30/03/2023 22:45:28	27/04/2023
IMMU - BackupD2023-03-29T224524_782C.vib	14.8 GB	6.57 GB	1.1 x	2.0 x	29/03/2023 22:45:24	27/04/2023
IMMU - BackupD2023-03-28T224506_DAB8.vib	16.0 GB	7.25 GB	1.1 x	2.0 x	28/03/2023 22:45:06	27/04/2023
IMMU - BackupD2023-03-27T224512_B28B.vib	18.1 GB	8.62 GB	1.0 x	2.0 x	27/03/2023 22:45:12	27/04/2023
IMMU - BackupD2023-03-26T224504_0E6D.vib	13.8 GB	6.67 GB	1.0 x	2.1 x	26/03/2023 22:45:04	27/04/2023
IMMU - BackupD2023-03-25T224523_AAE7.vib	10.2 GB	4.57 GB	1.0 x	2.2 x	25/03/2023 22:45:23	27/04/2023

Backup size: 7.63 TB

Historical layout



Data management protection strategy



veeAM





Thank you

veeAMON2023