VEEAMON 2023

How Ryanair Achieved Operational Resiliency Through Fortified Backups

Paul Walsh

Senior Systems Engineer

Ryanair

Rasmus Haslund

Principal Technologist

Veeam Software

505

aircraft for summer 2022

210

'Gamechangers'
on order
197 seats

409

B737-Next Gen
189 seats

29

Airbus A320s
180 seats

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

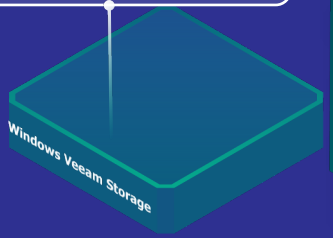
Head office VMware
- AD integrated VMWare farm.
- Multiple Large VLANs.
- Sporadic Windows/Linux firewall rules.

Link to DR site
- Slow 1GB link to DR.
- Stretched VLANs.

DR VMWare farm
- AD integrated VMWare farm.
- Multiple large stretched VLANs.
- Sporadic Windows/Linux firewall rules.

Veeam infrastructure
- 2X large storage repositories.
- AD domain integrated Veeam® console.
- AD domain integrated repos.
- Reverse incremental to NTFS.
- Backup console located in HQ as a VM.
- Shared VLAN with PROD servers.

Veeam infrastructure
- 2X large storage repositories.
- AD domain integrated repos.
- Backup copies to NTFS.
- Backup console located in HQ as a VM.
- Shared VLAN with PROD servers.
- Replicas from source VM.



VEEAMON 2023

Backups are target #1

What is an immutable backup?

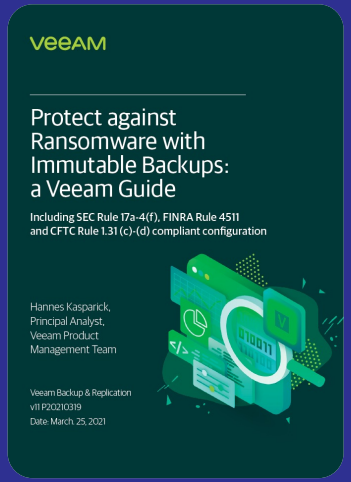
Preventing deletion of blocks of data or associated metadata until the expiration date set is met

A compliant hardened repository

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

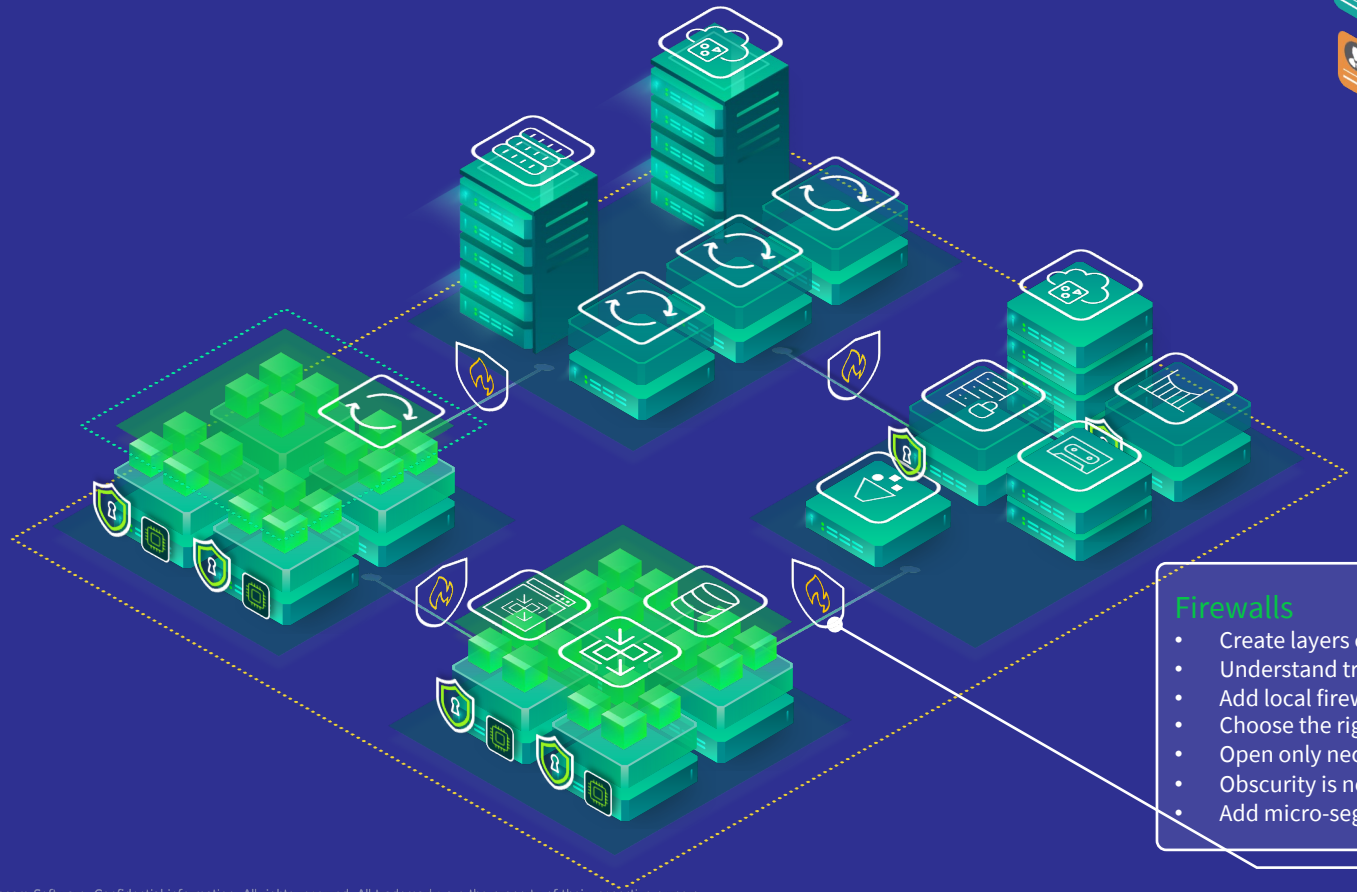
https://www.veeam.com/compliance-assessment-report-cohasset_wpp.pdf

White paper for IT professionals (Veeam administrators)



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

Network fortification



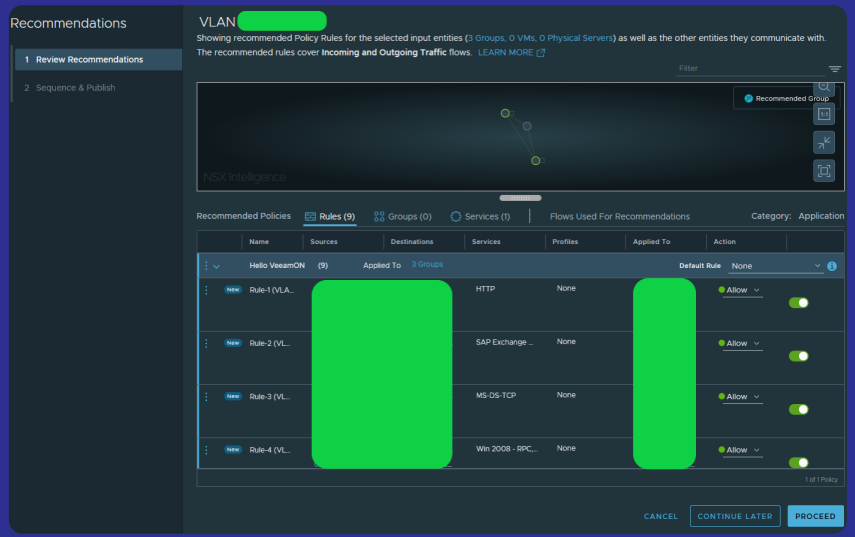
Firewalls

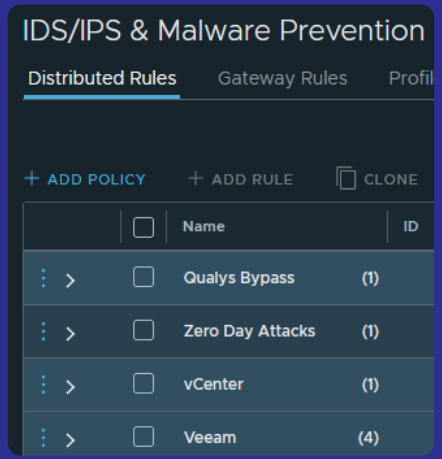
- Create layers of defense.
- Understand traffic flows.
- Add local firewalls (ring of fire).
- Choose the right firewall type.
- Open only necessary ports.
- Obscurity is no security.
- Add micro-segmentation.

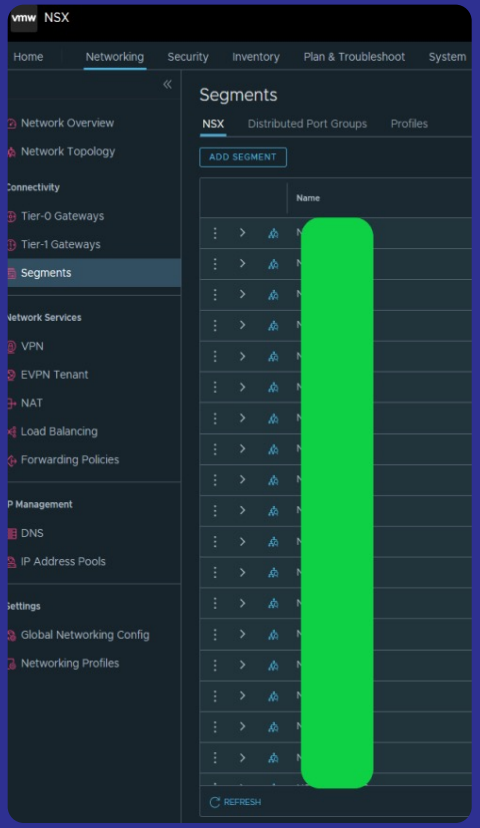
Network fortification

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.







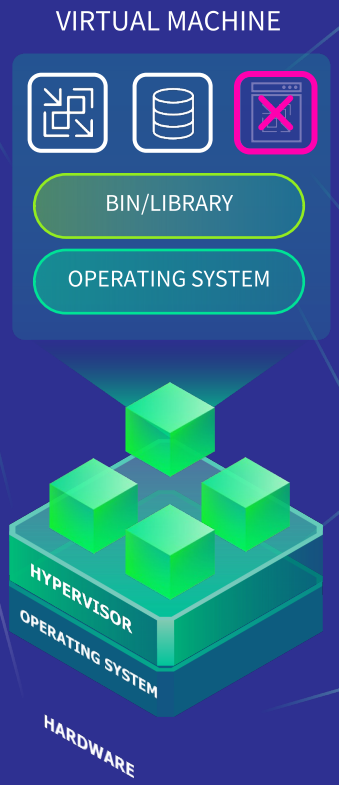
Backup server

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.



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 V12**).
5. Enable auto logoff (**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.

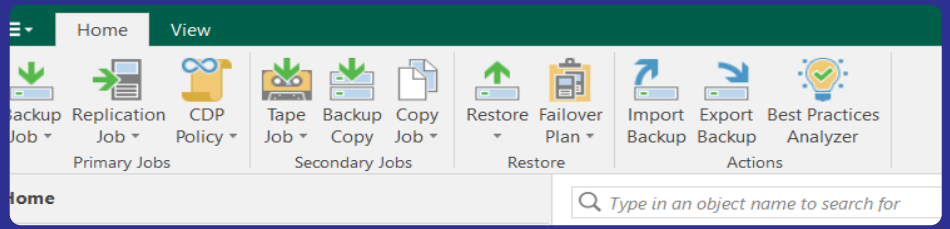
Regular update & patch
- Hypervisor.
- VM operating system.
- App Veeam Backup & Replication™.

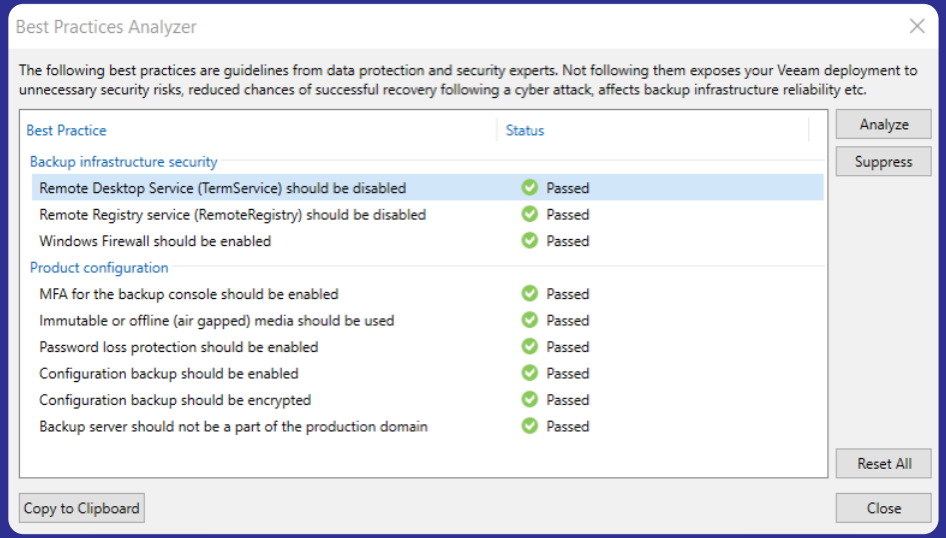
Segmentation
- Zone: management.
- Network: back-end management.
- Domain: management (Kerberos).
- Firewall: on edge (traffic rules).

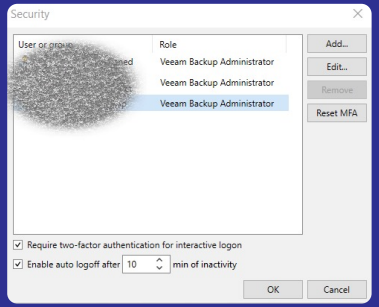
VEEAMON 2023

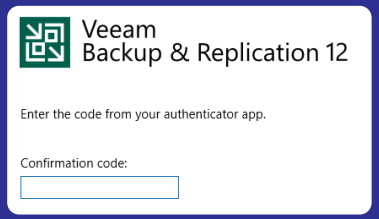
Veeam Console Best Practices

- 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.









Repository server

Lockdown

- Disable/remove unnecessary features.
- Use 2FA to access the repository server.
- Limit port access (firewall) when available.

Regular update & patch

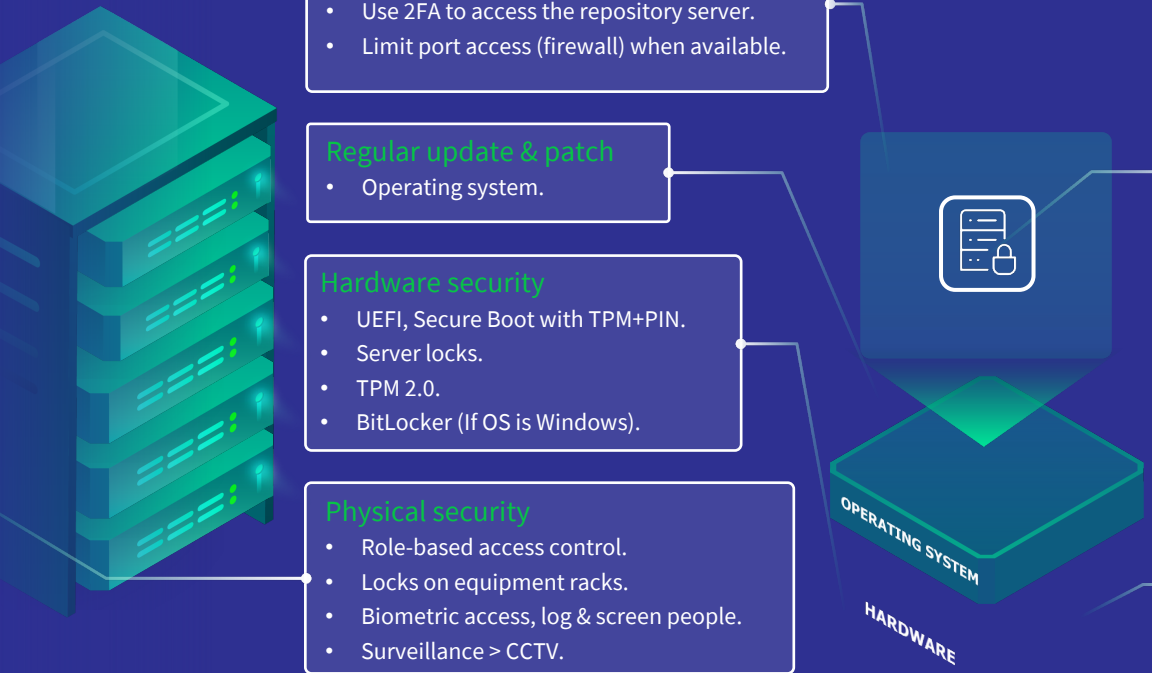
- Operating system.

Hardware security

- UEFI, Secure Boot with TPM+PIN.
- Server locks.
- TPM 2.0.
- BitLocker (If OS is Windows).

Physical security

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



Veeam Backup & Replication repository

1. Make sure the repo disk system is secure following vendor BPs (Data Domain, SAN Array, NAS).
2. Use immutable snapshots if available.
3. Use the Veeam hardened and immutable repo (Linux) where you can (zero trust).
4. Same domain user advice as with Veeam Backup & Replication.
5. Keep on an isolated zero trust backup network.
6. Keep off-site, air-gapped, immutable copies.

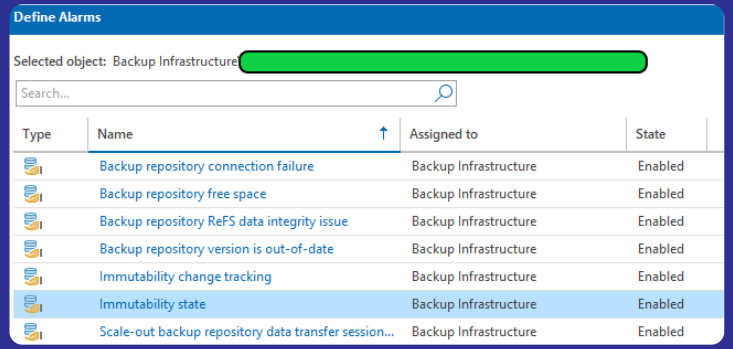
Segmentation

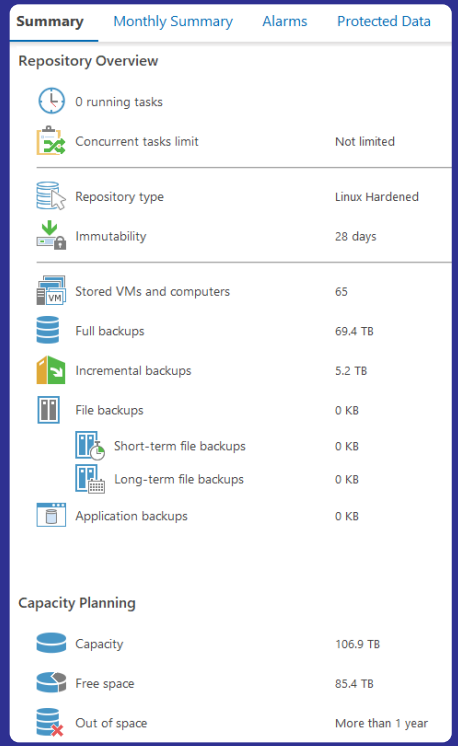
- Zone: restricted.
- Network: backup (IPv4 or IPv6).
- Domain: management (Kerberos).
- Firewall: on edge (traffic rules).

Repository server monitoring

Use Veeam ONE to monitor repository

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

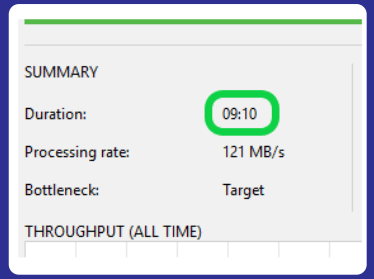


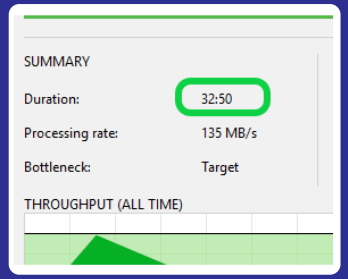


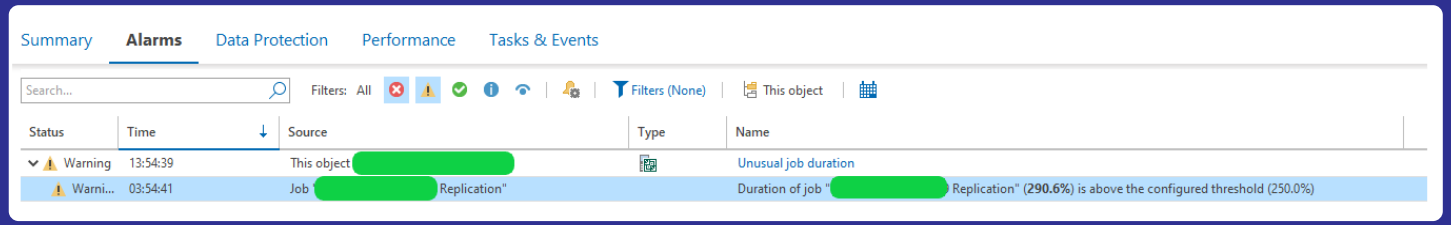
Backup job/copy job/replica monitoring

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.



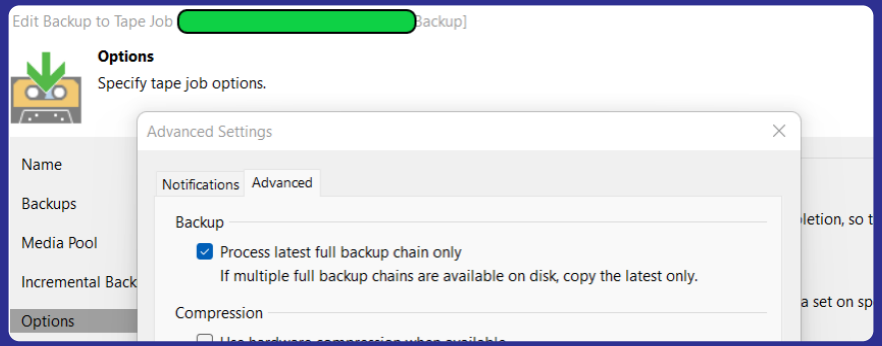




Long-term storage of data

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 - [redacted] 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 - [redacted] 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 - [redacted] 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 - [redacted] 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 - [redacted] BackupD2023-04-01T224509_FB47.vib	9.58 GB	4.14 GB	1.0 x	2.2 x	01/04/2023 22:45:09	03/05/2023
IMMU - [redacted] 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 - [redacted] 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 - [redacted] 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 - [redacted] 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 - [redacted] 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 - [redacted] 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 - [redacted] 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

Off-site air-gapped backups
- AWS VTL archive.

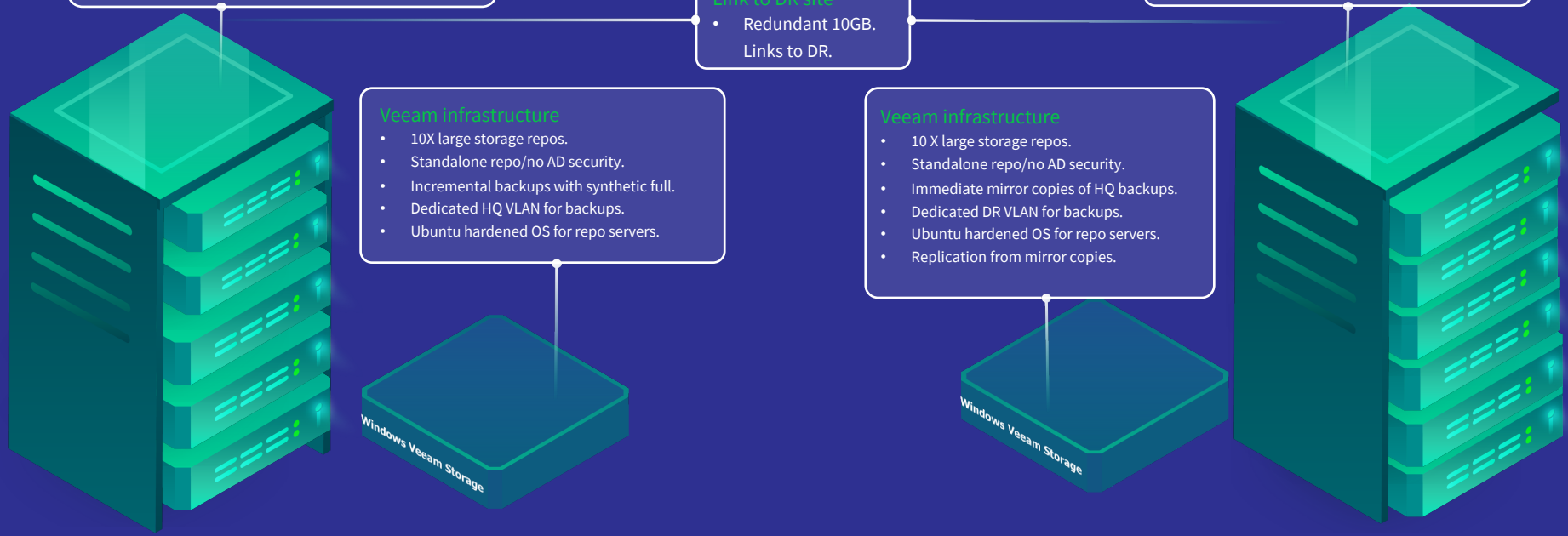
Head office VMware
- AD integrated VMWare farm.
- Multiple small NSX Segments.
- Domain controlled Windows firewall policies.
- NSX firewall on each segment for E/W traffic.
- Physical firewalls for N/S traffic.

Link to DR site
- Redundant 10GB. Links to DR.

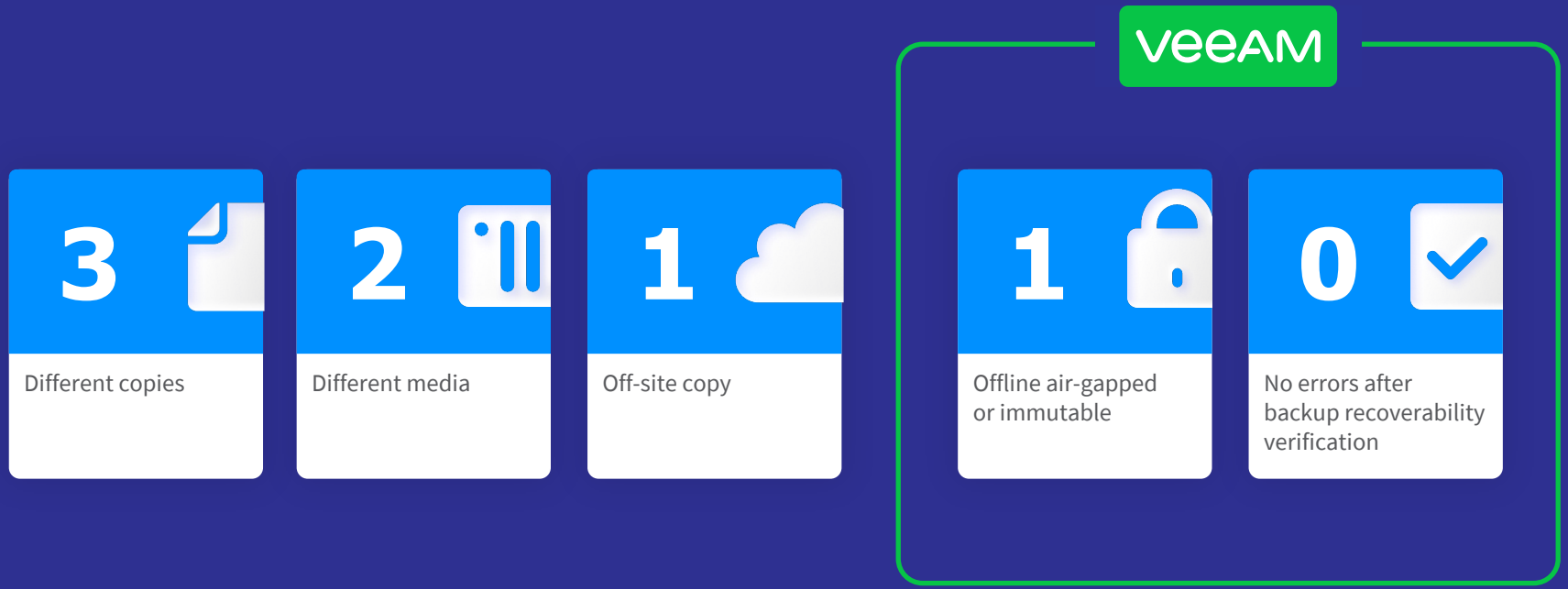
DR VMware
- Standalone VMWare farm.
- Multiple small NSX segments.
- Domain controlled Windows firewall policies.
- NSX Firewall on each segment for E/W traffic.
- Physical Firewalls for N/S traffic.

Veeam infrastructure
- 10X large storage repos.
- Standalone repo/no AD security.
- Incremental backups with synthetic full.
- Dedicated HQ VLAN for backups.
- Ubuntu hardened OS for repo servers.

Veeam infrastructure
- 10 X large storage repos.
- Standalone repo/no AD security.
- Immediate mirror copies of HQ backups.
- Dedicated DR VLAN for backups.
- Ubuntu hardened OS for repo servers.
- Replication from mirror copies.



Data management protection strategy




Thank you
VEEAMON 2023