

Veeam – So schützen Sie sich vor Ransomware



Alex Berndt

Systems Engineer

Veeam Data Platform

Proven Recovery Orchestration

Proactive Monitoring and Analytics

Secure Backup and Fast Recovery

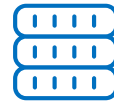
Native APIs



Cloud



Virtual



Physical



Apps



SaaS

PLATFORM
EXTENSIONS

Microsoft 365



aws

Azure

Google Cloud

kubernetes

On-Premises | In the Cloud | XaaS

Häufigkeit von Ransomware-Vorfällen

Von wie vielen Ransomware-Angriffen war Ihre Organisation in den letzten 12 Monaten betroffen? (n = 1.932)

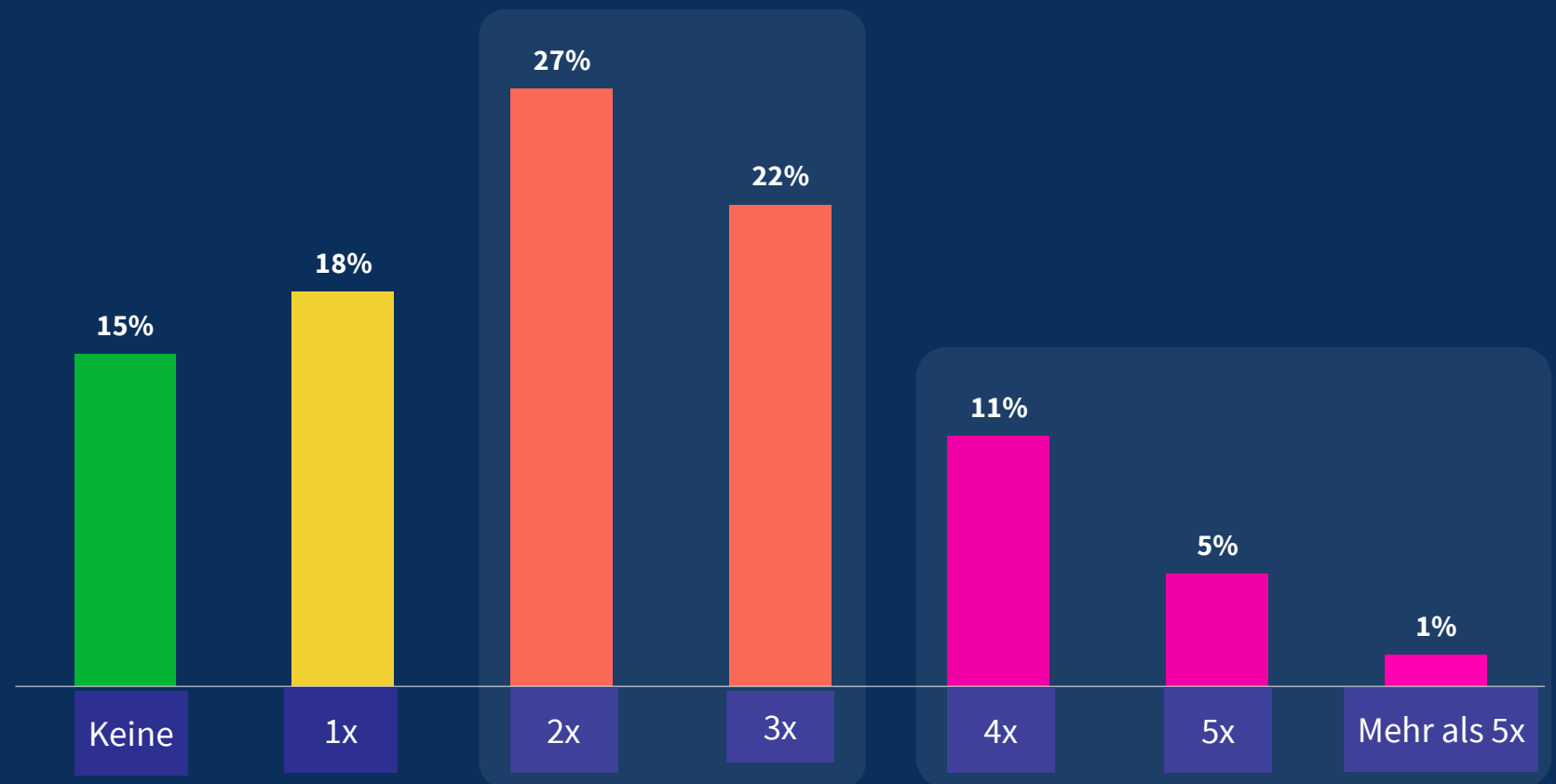
85%

der Organisationen waren mindestens einmal von Ransomware betroffen.

Die Anzahl derer, die von vier oder mehr Angriffen betroffen waren (17%), war größer als derer, die von überhaupt nicht attackiert wurden (15%).

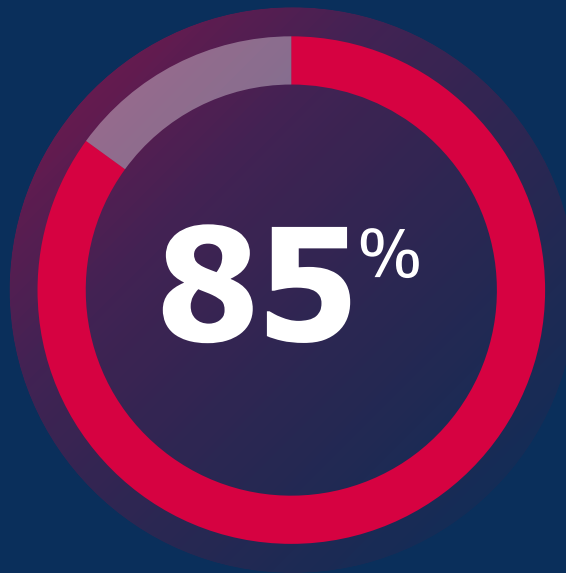
49%

der Organisationen waren von zwei oder drei Angriffen betroffen.



Quelle: Data Protection Trends Report 2023
<https://vee.am/DPR23>

Ransomware is the worst kind of disaster



of organizations experienced at least 1 ransomware attack in the past year*



of organizations were able to recover without paying the ransom**



Organizations paid the ransom and never got their data back**

*2023 Veeam Data Protection Report; **2023 Veeam Ransomware Trends Report

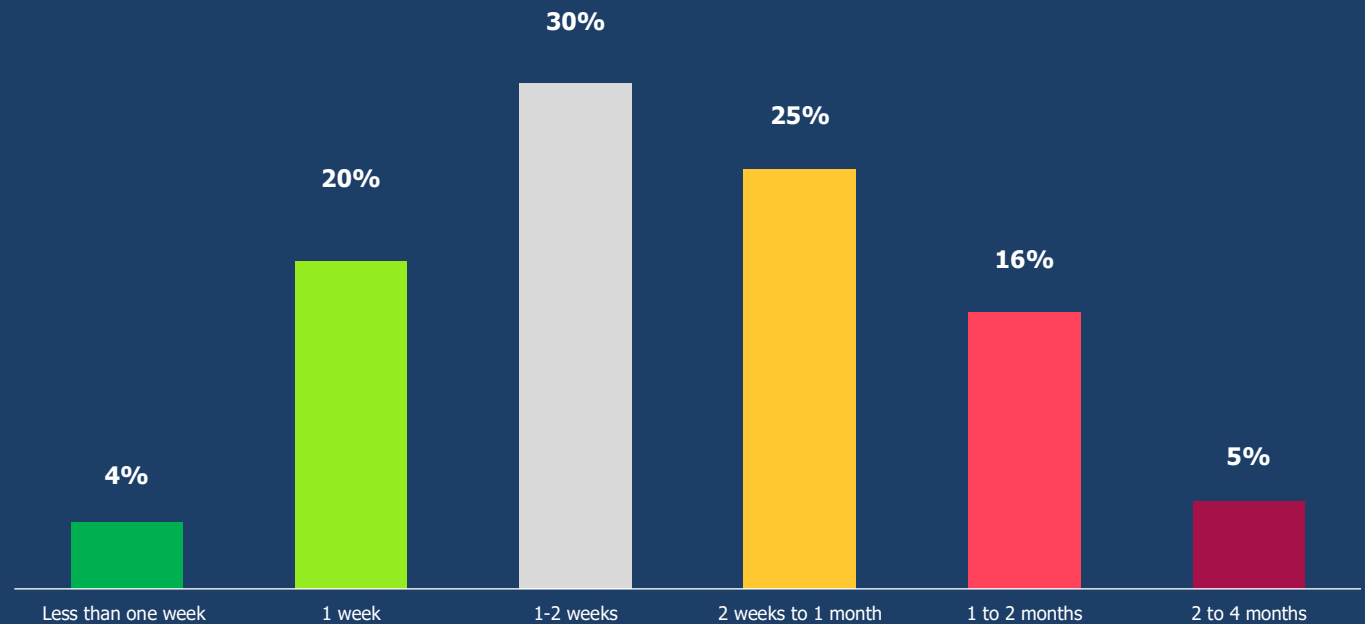
Recovery from ransomware is not easy



How long did recovery take?

It takes on average **three weeks** to recover (per attack) – after triage

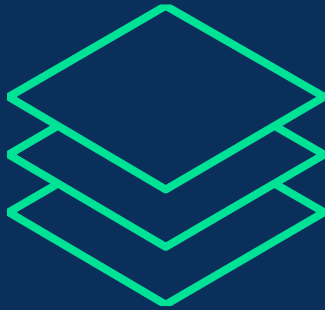
How long did the entire remediation/recovery take before the organization at large would say the event was "over"?*



*Source: 2023 Ransomware Trends Report 2023

Schutz der Backup-Infrastruktur

Abwehr von Ransomware

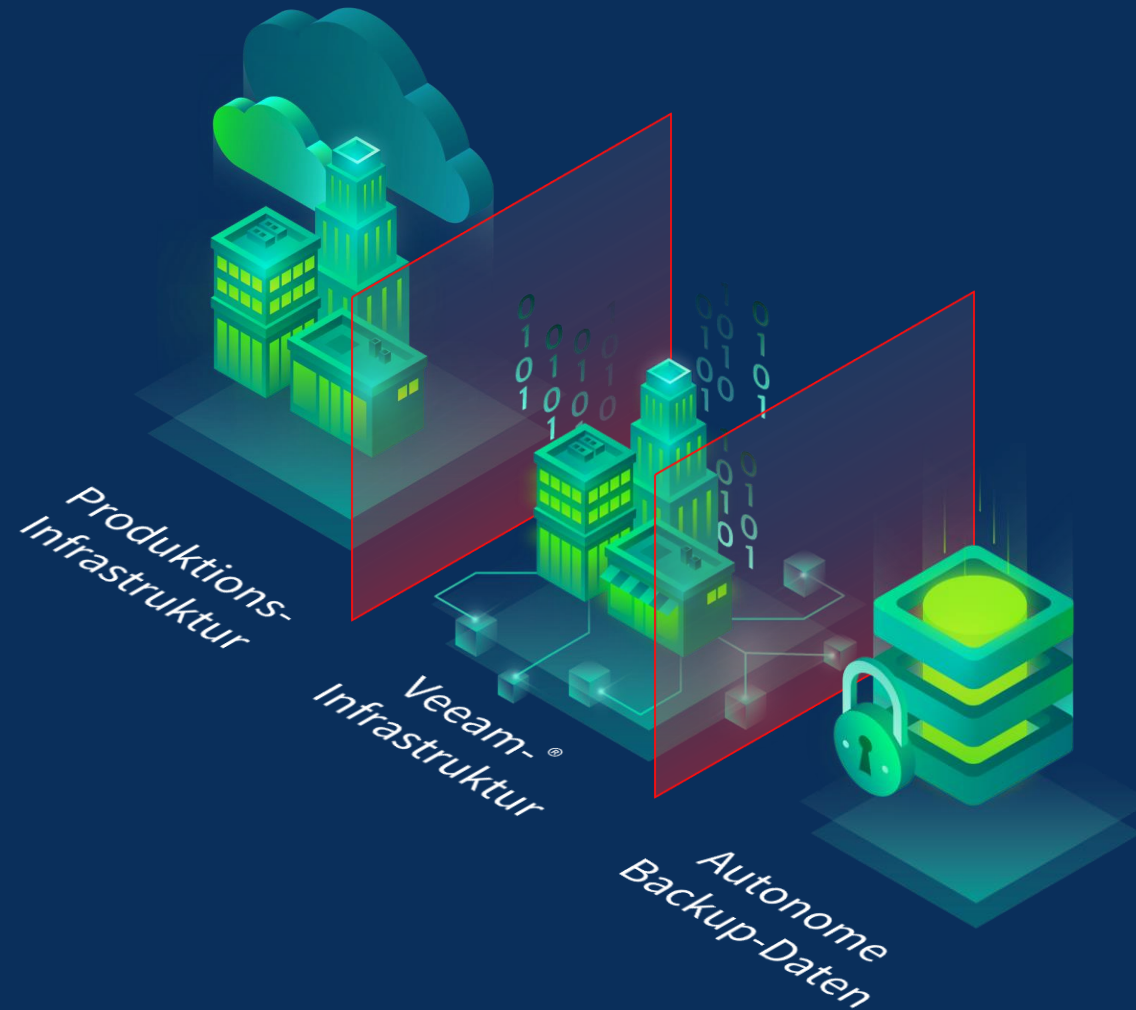


Mehrstufiger
Schutz



Es gibt keinen
Königsweg

Cyberresilienzbereiche

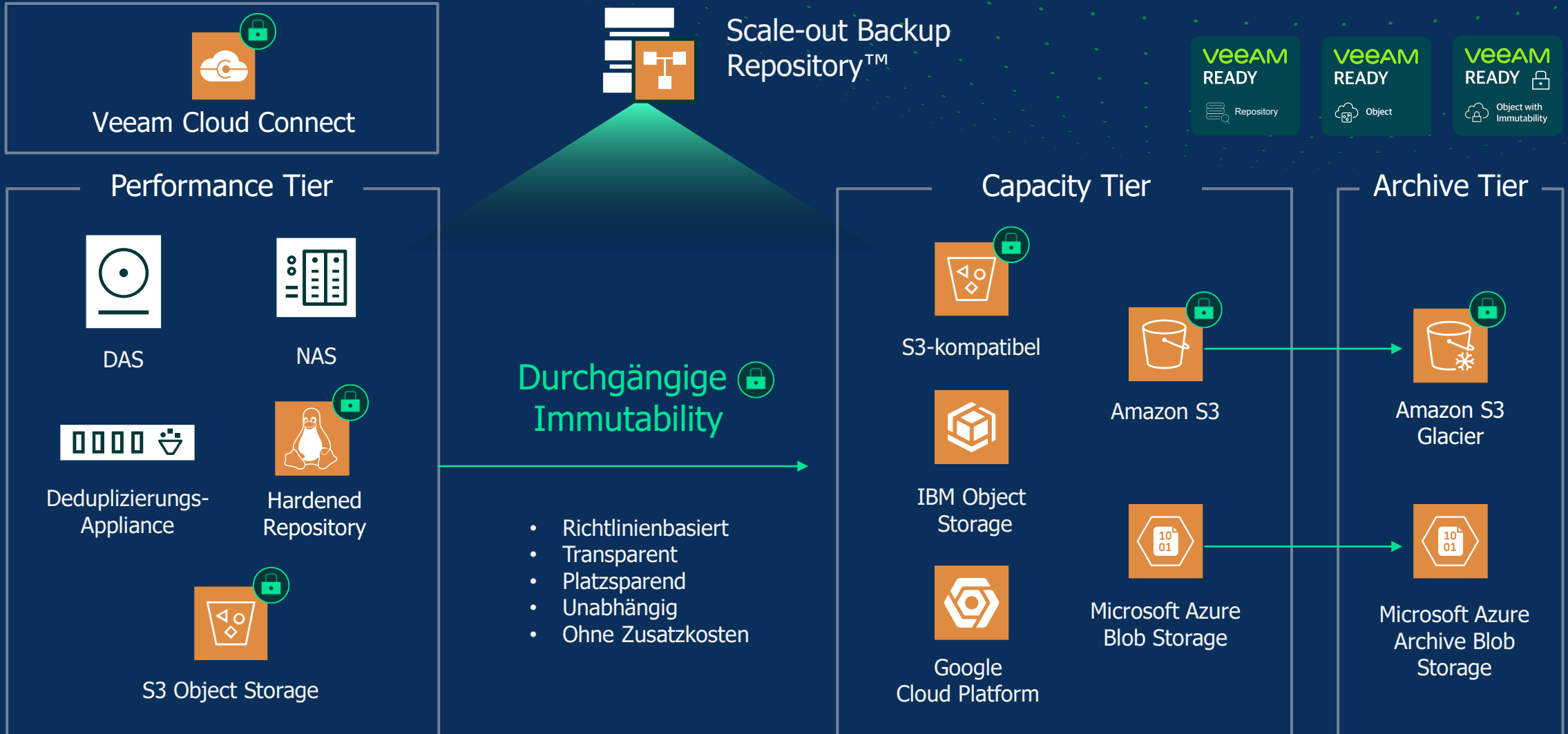


Immutable

Verschlüsselt

3-2-1-1-0

Durchgängige Immutability



NIST- konformes

Cybersicherheits-
Framework



veeam



Identifikation

Tracking und Auditing
von Änderungen

Intelligente
Diagnosefunktionen



Schutz

DataLabs – Patch-
Management-Forensik

Kontinuierliche
Datensicherung (CDP)

Veeam Disaster Recovery
Orchestrator

Sichere Wiederherstellung
(Secure Restore)

Mehrstufige
Wiederherstellung
(Staged Restore)



Erkennung

Veeam® DataLabs™

API für die
Datenintegration



Reaktion

Unveränderlicher

Speicher

Unveränderlicher Cloud-
Speicher

Verschlüsselung
und Schutz

Snapshot-
Orchestrierung

Moderne
Datensicherung



Wieder- herstellung

Sofortige

Wiederherstellungen



Ransomware Erkennung

Seit über 5 Jahren verfügt **Veeam ONE** über eine Logik, mit der Ransomware-Aktivitäten auf Produktions-Workloads erkannt werden können.

The screenshot displays the Veeam ONE interface. On the left is a navigation tree with categories like Hyper-V, Backup & Replication, and Internal. The main area shows a list of alarms. The 'Possible ransomware activity' alarm is selected and highlighted in blue. Below the list, the 'Alarm details' section is visible, containing information about the knowledge, cause, and resolution of the alarm.

Local volume free space	Predefined	Enabled	Virtual Infrastructure
Machine remoting system failure	Predefined	Enabled	Virtual Infrastructure
Missing latest cluster configuration data	Predefined	Enabled	Virtual Infrastructure
Network communication failure	Predefined	Enabled	Virtual Infrastructure
No disk space to run this VM	Predefined	Enabled	Virtual Infrastructure
Not enough memory to start a VM	Predefined	Enabled	Virtual Infrastructure
Possible ransomware activity	Predefined	Enabled	Virtual Infrastructure

Alarm details

Knowledge
Veeam ONE detected suspicious activity on this VM

Cause
This Virtual Machine had high write rate on datastore along with high CPU Usage which can be caused by ransomware activity

Resolution
Check if files on VM are encrypted by ransomware. Run up-to-date security software, prevent ransomware propagation, ask for qualified assistance if needed backup in a case the files cannot be repaired. If VM was not affected by ransomware, raise the alarm thresholds.

Sichere Workload-Tests

Regelmäßiges Testen aller gesicherten Workloads und DR-Szenarien

Sind die Backups virenfrei?

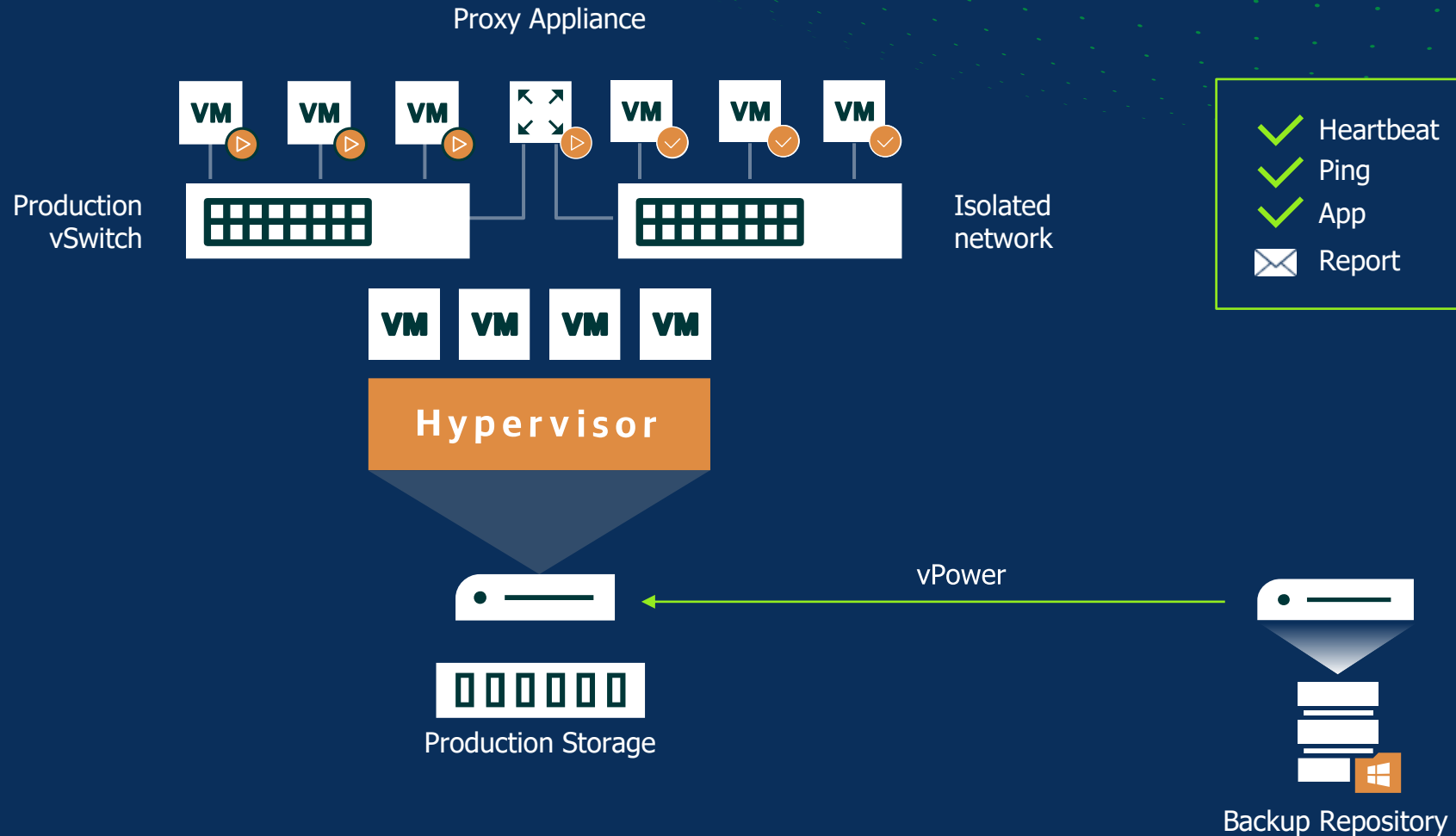
- Überprüfung mit aktuellen Virenschanner-Definitionen

~~Never~~ change a running system!

- Regelmäßiges Einspielen von Patches und Updates



Überprüfung der Backups



Sicherer Zugang

- Verhinderung von unberechtigtem Zugriff
- Aktivieren Sie MFA
- Aktivieren Sie die automatische Abmeldung bei Inaktivität
- Verwenden Sie rollenbasierte Zugriffskontrollen (RBAC)
- Protokollierung und Meldung jedes Zugriffs

The illustration shows a data center environment with server racks and a cloud icon. Two windows are overlaid on the scene:

Veeam Backup & Replication 12 window:

Two-factor authentication has been enabled on this backup server.

Step 1. Open an authenticator app of your choice
Step 2. Scan QR code or enter:

Step 3. Click Next

Buttons: Save shortcut, Next, Close

Security window:

User or group	Role	
TECH\alison.summers	Veeam Backup Administrator	Add...
TECH\audrey.allen	Veeam Restore Operator	Edit...
TECH\madison.gray	Veeam Backup Operator	Remove

Veeam Backup and Replication dialog:

The user will be required to reconfigure MFA upon the next logon. Proceed?

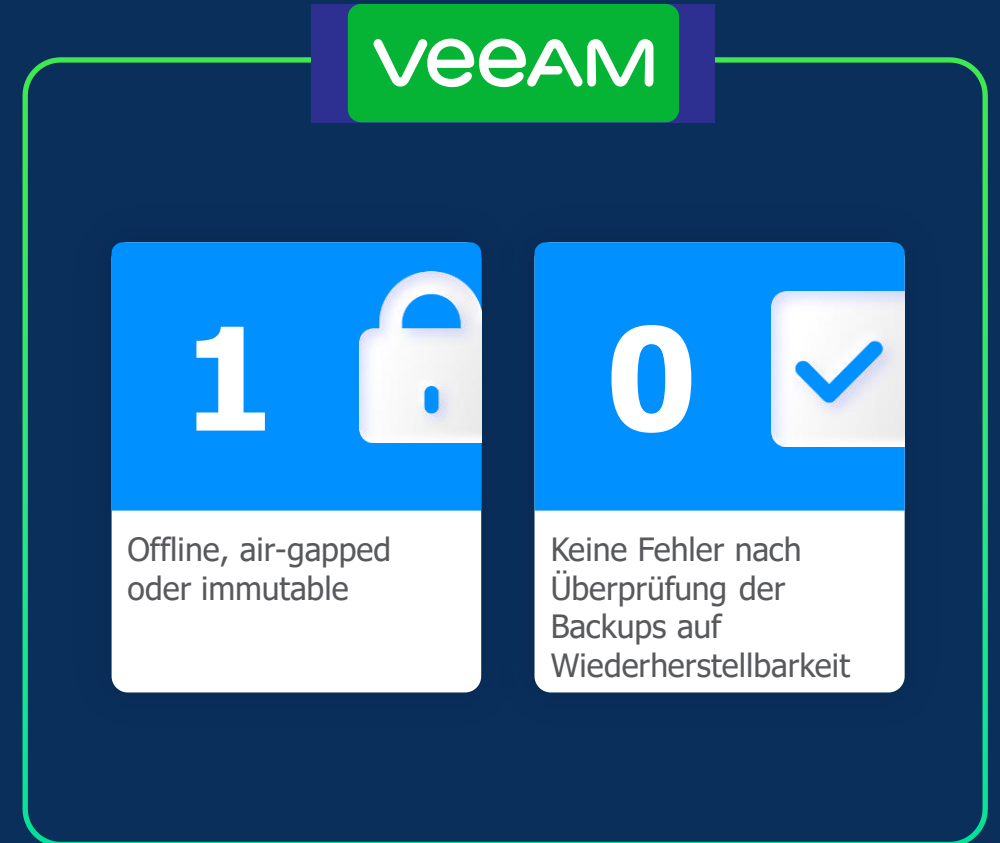
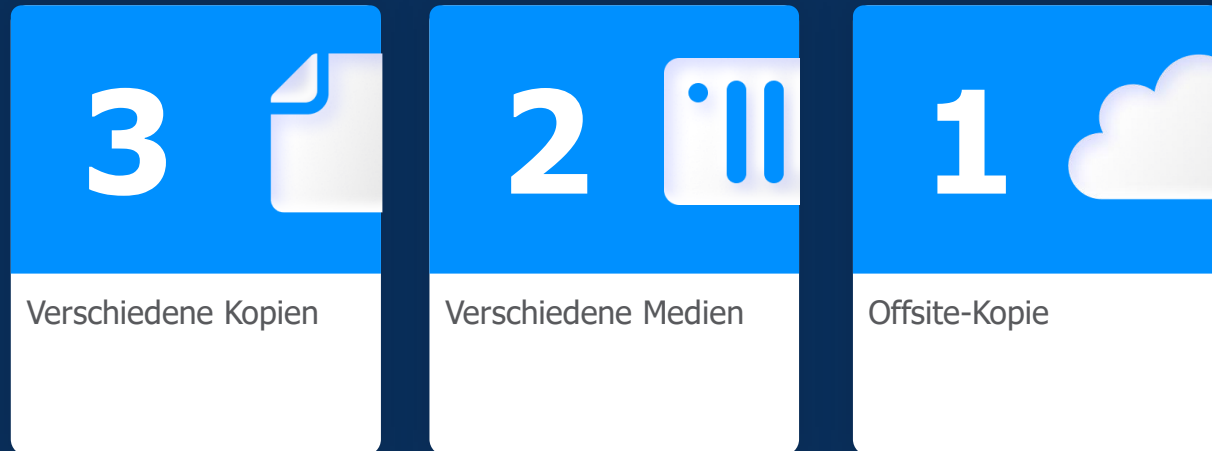
Buttons: OK, Cancel

Options:

- Require two-factor authentication for interactive logon
- Enable auto logoff after 10 min of inactivity

Buttons: OK, Cancel

Vorbereitet sein: die Datenschutz-Postleitzahl



Offline, immutable & air-gapped

Likely the single most-effective resiliency technique is to have some form of offline storage tape, removable disk, etc. as an **ultra-resilient copy**.

Media type	Characteristic
Tape media	Completely offline when not being written to or read from and WORM
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 +Insider Protection	Not connected directly to the backup infrastructure and use 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)
Immutable backups	Backups in AWS S3 and some S3-Compatible storage can keep backup data immutable
Hardened Linux Repository	Linux immutable flag on Veeam backups

Hardened Linux Repository – Überblick

Warum?

Vor Malware geschützte Repositories

Bei richtiger Konfiguration:
Schutz vor internen Bedrohungen

Was?

Backups sind nicht löschar

Wie?

Verwendung des „immutable“-
Dateisystemattributs unter Linux

Removing backup

Name: **Backup Deletion Job** Status: **Warning**
Action type: Backup Deletion Start time: 29.10.2020 11:32:48
Initiated by: LAB\administrator End time: 29.10.2020 11:33:18

Log

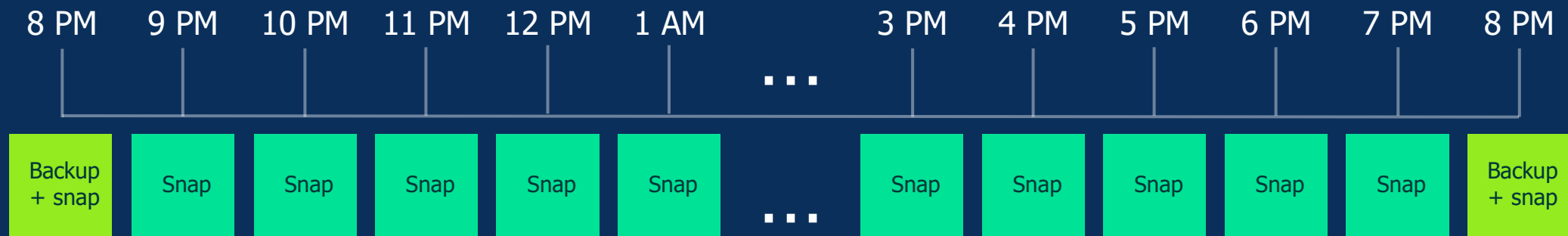
Message	Duration
✓ Starting backup deletion job	
✓ [TBD] Preparing entities for deletion	
✓ [TBD] Building deletion tasks	
✓ [TBD] Processed 1 of 1 entities (100% done)	0:00:26
! [BJ-hard1-7d-per-vm] Backup deleted with warning	0:00:23
! [TBD] Failed to delete immutable storages. Count: 4.	
! [TBD] Backup can be deleted after 09.11.2020 11:22	
✓ hard1-per-vm-chains-7days: 0 deleted, 0 skipped, 1 warned, 0 failed	
! Job finished with warning at 29.10.2020 11:33:18	

```
172.21.239.13 - KITTY
root@multistorage:/mnt/nfs/backups/BJ-immutable# lsattr -a
----- ./.
----- ./..
-i----- ./HK-Nano.vm-5636D2020-06-18T142332_7FC7.vbk
-i----- ./HK-Nano.vm-5636D2020-06-24T145659_5C3E.vib
-i----- ./veeam.0.lock
----- ./BJ-immutable.vbm
root@multistorage:/mnt/nfs/backups/BJ-immutable#
```

Use of Storage Snapshots for better RTO and RPO

During backup, data transport and consistency processing reduce performance of applications.

Leverage storage snapshots between the backup for even better Recovery Time and Recovery Point Objectives.



Wiederherstellung

Instant Recovery für alle Workloads

File-level recovery (Windows)	V2V conversion to vSphere/Hyper-V	Full VM restore	VM files restore	Multi-VM Instant Recovery	VM hard disk restore
Failover to a replica VM	File-level recovery (Multi-OS)	Quick Rollback	U-AIR restore	Restore from a replica VM	Replicate VM from a backup
General options		Instant VM disk recovery	Staged Restore	Secure Restore	Data Integration API
Veeam Explorers		Instant first-class disk recovery	Instant DB recovery		
Active Directory		Exchange		Teams	
Export container/object	Restore system objects/GPO	Save data	Send data	Save file/as ZIP	Send post/file
Restore a deleted container/object	Restore a changed container/object	Restore folder/item/mailbox	Export to PST file	Restore team/channel/tab/post/file	Export post
SharePoint		OneDrive		Oracle	
Save library/document	Send library/document	Save folder/document	Send document	Restore the latest state	Restore to a specific point in time
Restore library/list/document/site	Export library	Restore folder/document	Copy data to same/different user	Restore to a specific transaction	Restore from Oracle RMAN backup
SQL					
Restore the latest point	Restore to specific time/transaction	Restore/export DB schema	Export latest or point-in-time state	Publish latest or point-in-time state	Export as MDF/BAK

Agents			
Agent Backup to a Hyper-V VM	Guest OS files/folders/volumes	Agent Linux	Agent Windows
Agent Mac	Export a point as a virtual disk	P2C conversion	Application-level restore

vCloud Director			
Instant VM Recovery into vApp/vSphere	Full restore into vApp/vSphere	vCloud vApp restore	Linked Clone VMs to vCD

Tape			
Full VM to infrastructure	Files from tape	Backup from tape	Tenant restore

Network Shares		Restore entire file share	Rollback to a point in time
		Restore files and folders	Restore permissions and security attributes
		Instant share publishing	

91

Recovery scenarios with Veeam Backup & Replication v11

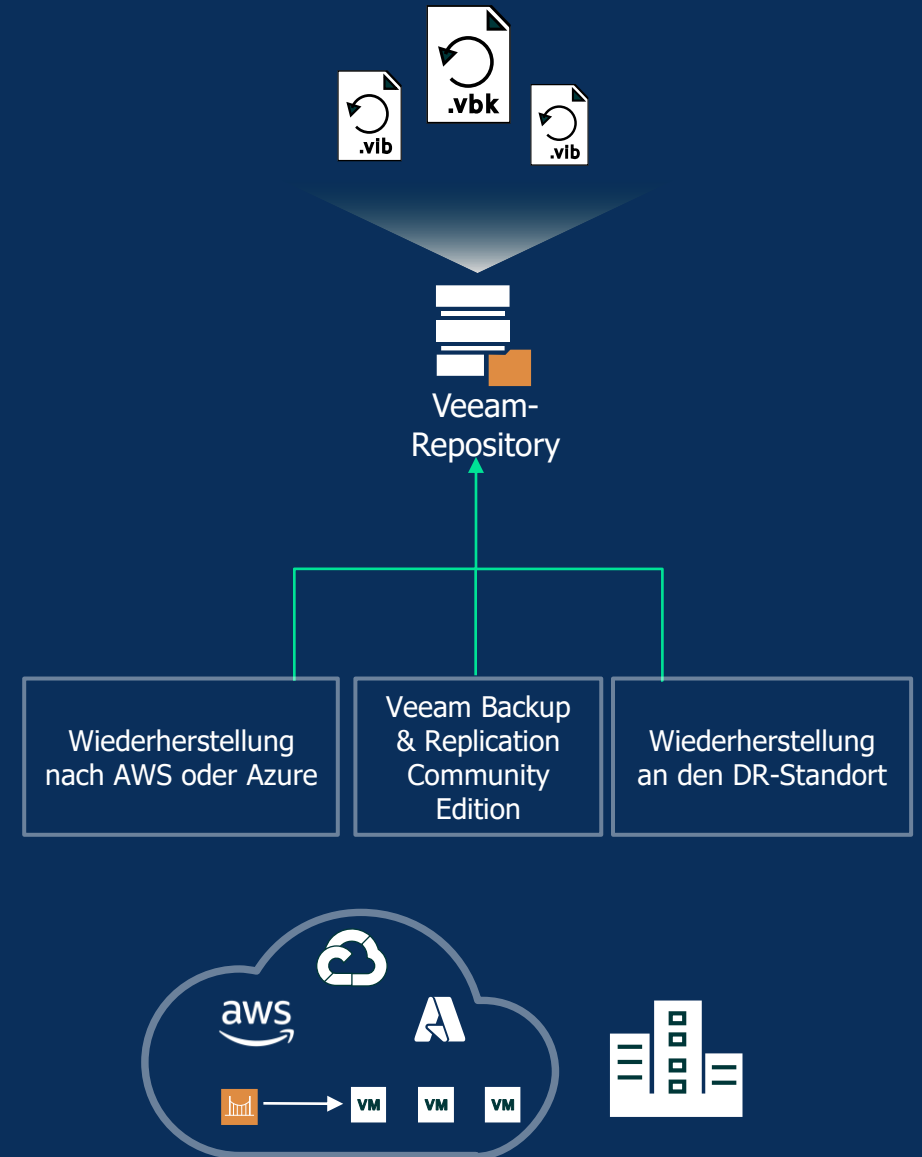
Backup Enterprise Manager			
1-click VM/file restore	Virtual disk restore	Launch failover plan	Restore of vCD infrastructure
Exchange item restore	SQL/Oracle DB restore	Self-service Restore Portal	Restore via RESTful API

Cloud			
Restore from "deleted" VCC backups	Restore from object storage	Restore from the VCC Provider	C2V conversion via "external" repo
		Partial/full site failover	Restore to Azure VM/AWS EC2

Explorer for Storage Snapshots			
Guest files (Windows/Multi-OS)	Instant VM/disk Recovery	SQL/Oracle DB restore	Exchange/SP/AD item restore

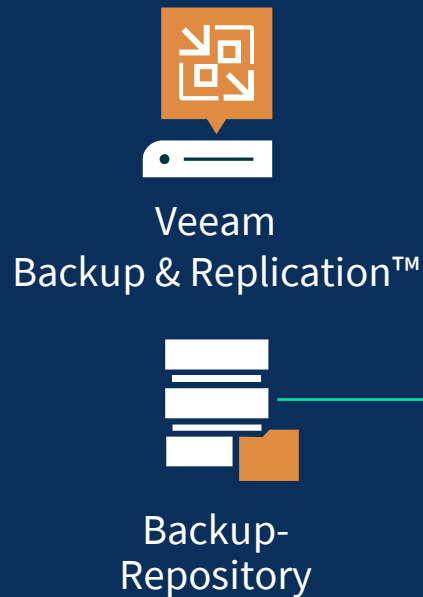
Datenmobilität

- ✓ Backups, Wiederherstellung und Migration auf, von oder innerhalb jeglicher Umgebungen mit einem vollständig übertragbaren Datenformat
- ✓ Modernisieren Sie Ihren Speicher durch Datenverschiebung, um das richtige Maß an Verfügbarkeit zu den geringsten Kosten zu erreichen
- ✓ Sorgen Sie für Datenflexibilität, um Daten jederzeit dorthin verschieben zu können, wo Sie sie brauchen – ohne Gebühren und über verschiedene Clouds hinweg.
- ✓ Gewährleistung der Business Continuity unabhängig vom Speicherort



Secure Restore

1. Wiederherstellungspunkt auswählen



2. Backup-Dateien direkt als Laufwerk einhängen

Antivirensoftware mit aktuellen Definitionen installiert

3. Antivirus-Check



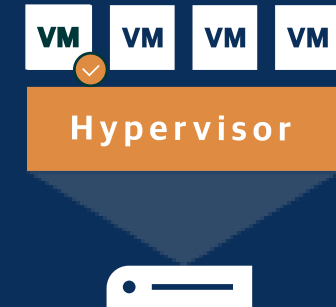
4a. Keine Infektion gefunden; Wiederherstellung fortsetzen



4b. Infektion gefunden; Wiederherstellung fortsetzen, aber Netzwerk trennen



4c. Infektion gefunden; Wiederherstellung stoppen



Microsoft Windows Defender



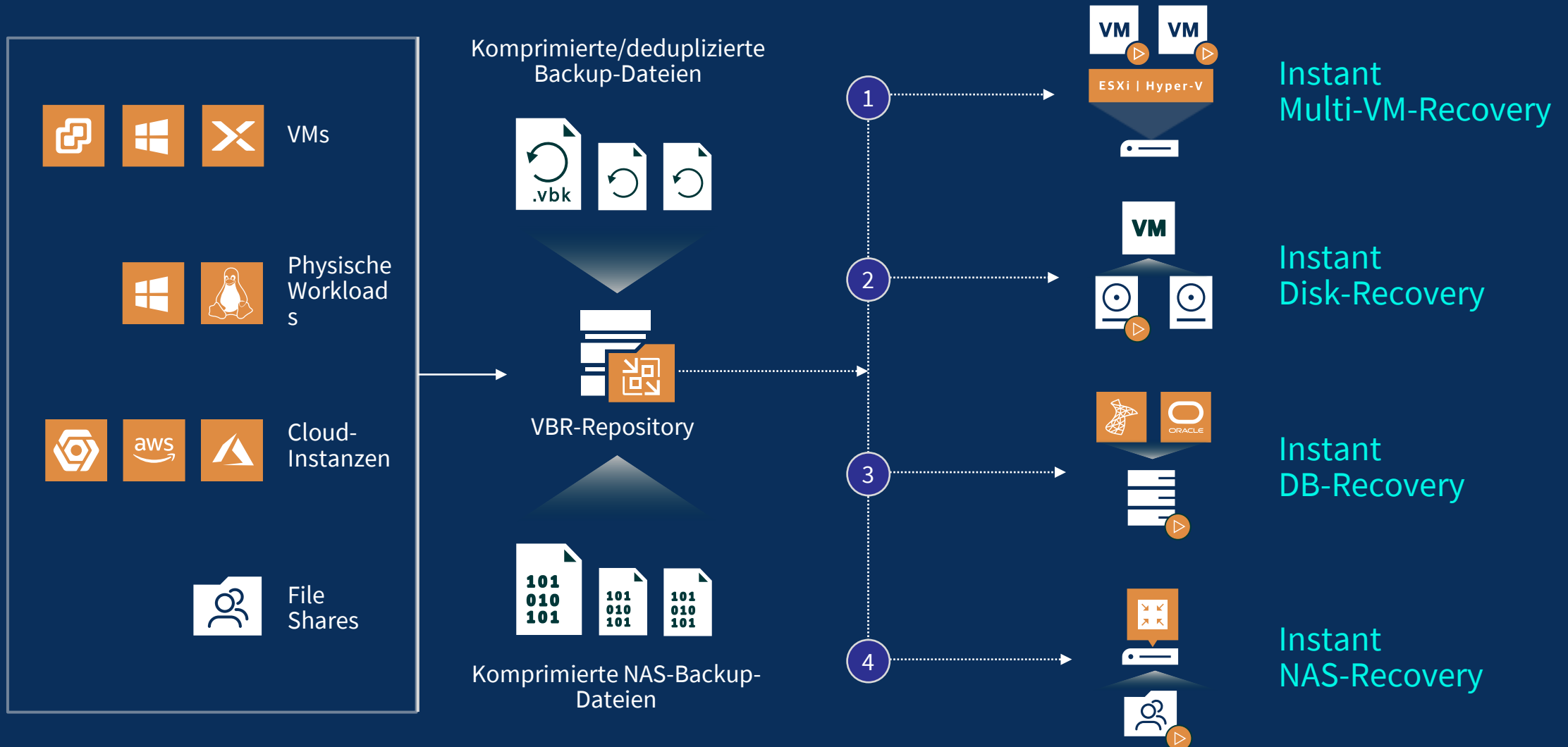
ESET NOD32 Smart Security



Symantec Protection Engine

Oder jede andere Antivirensoftware mit CMD-Unterstützung

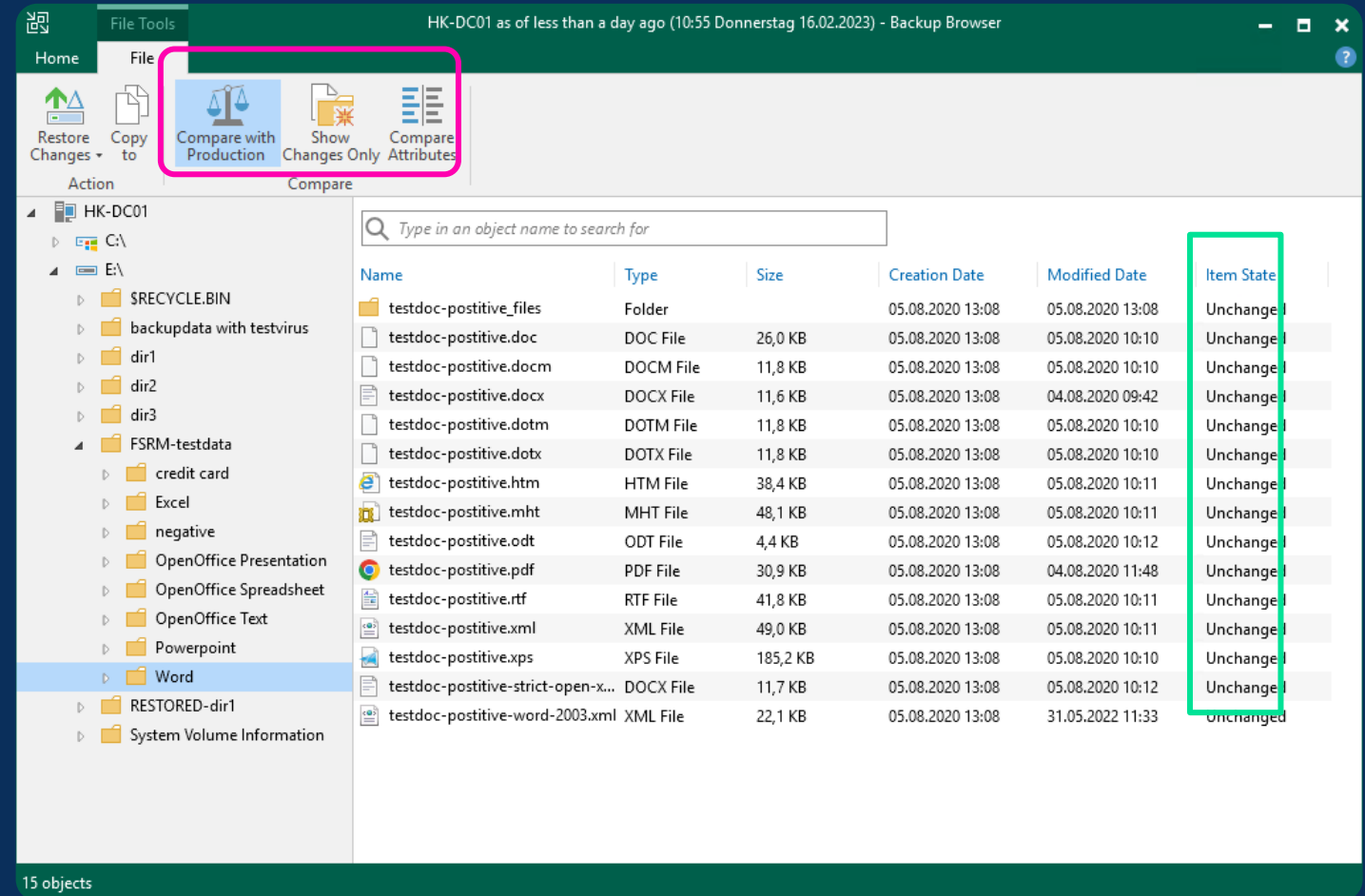
Instant Recovery „at Scale”



Einfach nur veränderte Dateien wiederherstellen

Windows File Explorer auf Dateiebene im Vergleich zur Produktion

Geänderte Objekte anzeigen, um potenziell verschlüsselte Dateien zu identifizieren



Veeam Explorer™ *for Microsoft Active Directory*

DLDC as of less than a day ago (12:57 PM Thursday 2/4/2021) - Veeam Explorer for Microsoft Active Directory

Home Container

Restore Container Export Container Compare Show Changed Objects Only Use LDAP Filter Search

Compare Active Directory objects with production
Compares objects state from backup with original Active Directory objects

Active Directory Databases

Name	Type
computer-Display	displaySpecifie
contact-Display	displaySpecifie
container-Display	displaySpecifie
default-Display	displaySpecifie
domainDNS-Display	displaySpecifie
domainPolicy-Display	displaySpecifie
DS-UI-Default-Settings	dSUISettings
foreignSecurityPrincipal-Display	displaySpecifie
group-Display	displaySpecifie
inetOrgPerson-Display	displaySpecifie
IntellimirrorGroup-Display	displaySpecifie
IntellimirrorSCP-Display	displaySpecifie
interSiteTransportContainer-Display	displaySpecifie
interSiteTransport-Display	displaySpecifie
licensingSiteSettings-Display	displaySpecifie
localPolicy-Display	displaySpecifie
lostAndFound-Display	displaySpecifie
msCOM-Partition-Display	displavSpecifie

Load completed 56 objects found.

DLDC as of less than a day ago (12:57 PM Thursday 2/4/2021) - Veeam Explorer for Microsoft Active Directory

Home Container

Restore Container Export Container Compare Show Changed Objects Only Use LDAP Filter Search

Active Directory Databases

Search 401

Name	Type	Item State	Description
computer-Display	displaySpecifie		
contact-Display	displaySpecifie		

Load completed 2 objects found.

veeam

Automatisierung, Test und Dokumentation von DR

Typische DR-Probleme



UNDOKUMENTIERT



UNGETESTET



UNZUVERLÄSSIG

- Komplexität
- Sehr hoher Zeit-/Ressourcenaufwand
- Fehleranfällig

Veeam Disaster Recovery Orchestrator



**DYNAMISCHE
DOKUMENTE**



UNGETESTET



UNZUVERLÄSSIG

- Automatisiert
- Anpassbar
- Nachvollziehbar („Audit Trail“)

Veeam Disaster Recovery Orchestrator



**DYNAMISCHE
DOKUMENTE**



**AUTOMATISIERTE
TESTS**



UNZUVERLÄSSIG

- Automatisiert
- Detaillierte Reports
- Keine Beeinträchtigung der produktiven Systeme

Veeam Disaster Recovery Orchestrator



**DYNAMISCHE
DOKUMENTE**



**AUTOMATISIERTE
TESTS**

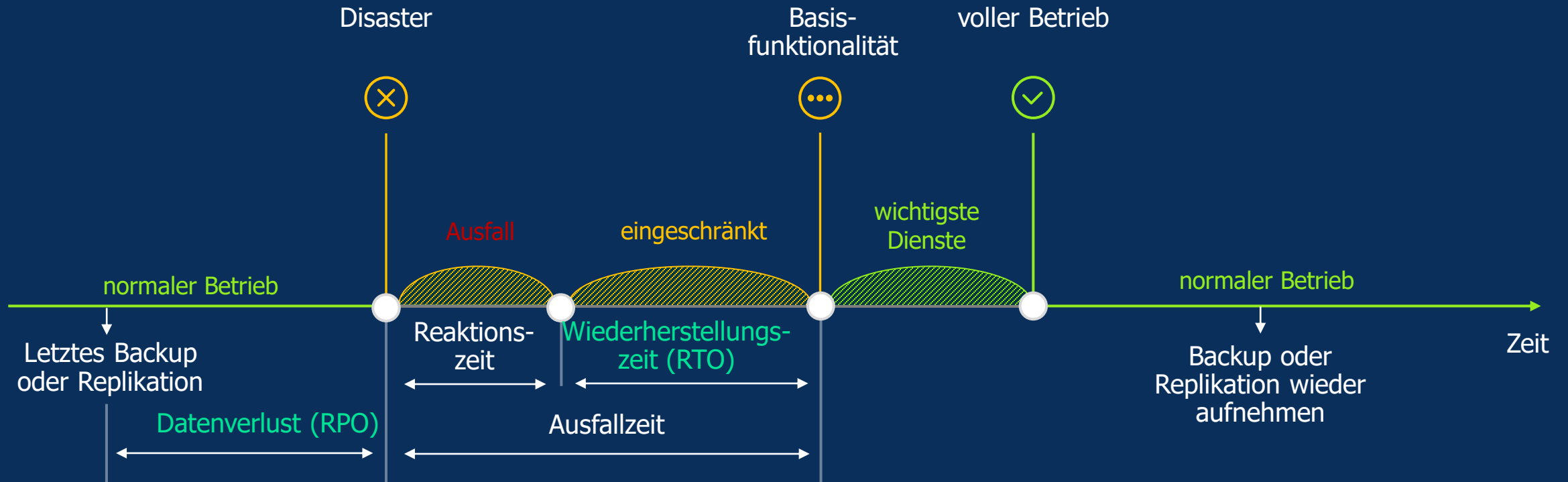


**ZUVERLÄSSIGE WIE-
DERHERSTELLUNG**

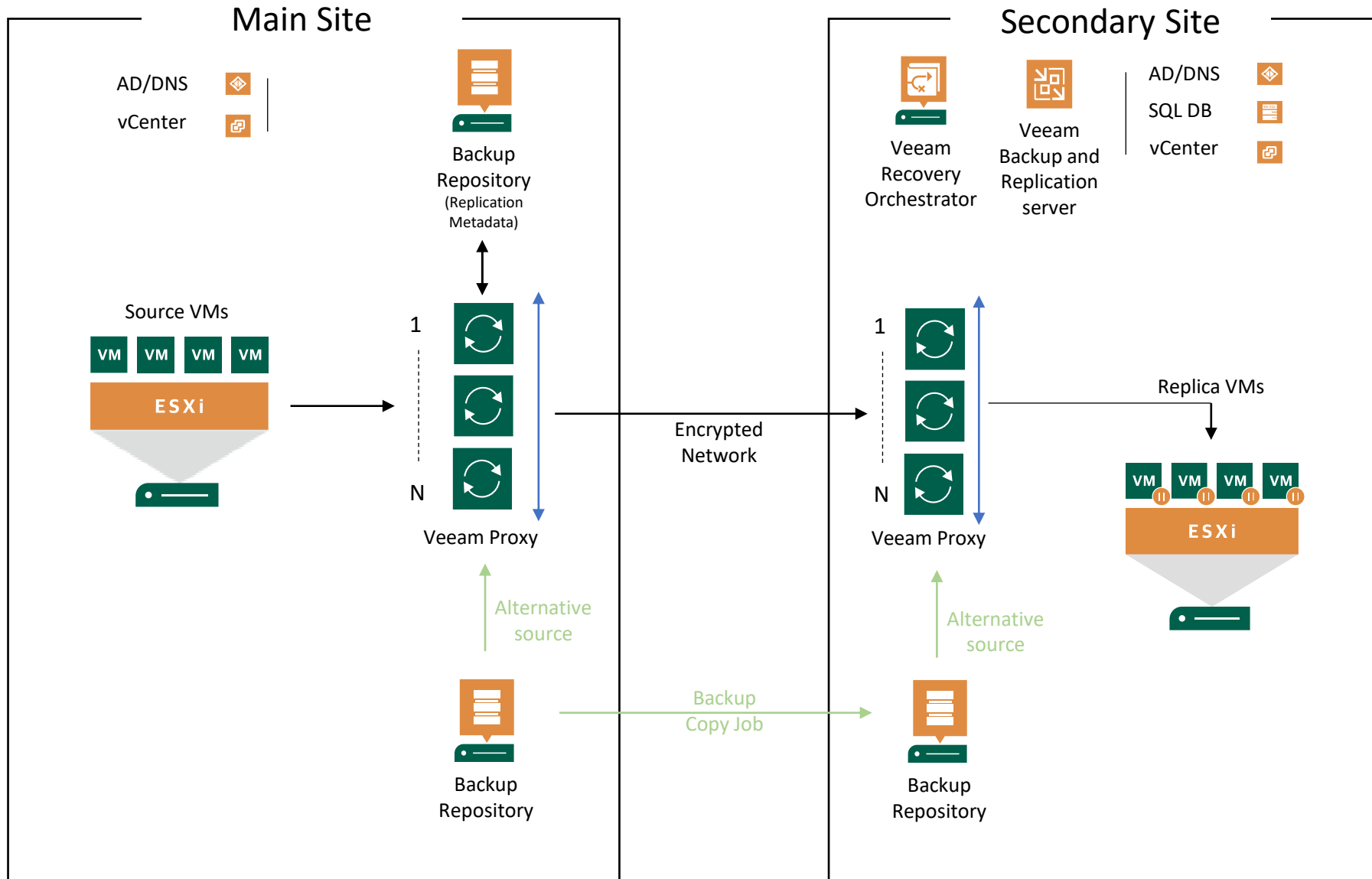
- Automatisiert
- Verifiziert
- Optimiert

Wiederherstellungsprozess

Was passiert, wenn eine Katastrophe eintritt?



Replica Example



V6 New Features



Cloud DR

Recover any backup as an **Azure** VM



Agent DR

Recover Veeam **Agent** backups as VMs



Clean DR

Scan for **ransomware** during recovery

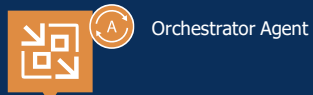
Clean DR



Veeam Recovery Orchestrator server



1. Select multiple restore point(s)

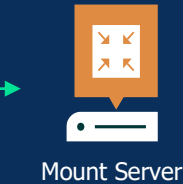


Orchestrator Agent

Veeam Backup & Replication



Backup repository



Mount Server

2. Mount disks directly from backup file to mount server

Anti-virus software installed with latest definitions

3. Anti-virus check

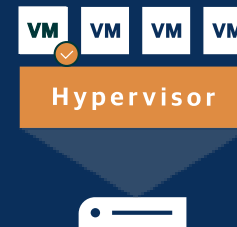


4a. No infections found; continue restore

4b. Infection found; proceed to next available restore point



4c. Infection found; stop restore or complete restore and connect VM to a quarantine network



Hypervisor



Veeam Recovery Orchestrator



Dynamic Documentation

Automatically updated reports for checks, tests and executions help correct issues with DR readiness



Zero-Impact Testing

DataLab tests increase confidence, simulating disaster recovery without impacting production systems



Compliance

RTO and RPO reporting help meet compliance standards and SLA targets



1-Click Recovery At Scale

Recover single apps or an entire site with one click, secured by role-based access control

Supported platforms and applications:



Azure, vSphere



Agents:
Windows & Linux



Apps:
Exchange, SQL, SharePoint



Storage:
NetApp, HPE, Lenovo



Custom scripting

Lizenzierung

Veeam Data Platform Packages

Platform Editions	Backup and Recovery	Monitoring and Analytics	Recovery Orchestration	Ransomware Warranty (add-on)
Premium	✓	✓	✓	✓
Advanced	✓	✓		
Foundation	✓			
Essentials	✓	✓		
<i>Supporting product components</i>	Veeam Backup & Replication	Veeam ONE	Veeam Recovery Orchestrator	

Also Available:

- Veeam Backup & Replication Community Edition

Q&A

The image features a central logo for Veeam. The logo consists of the word "veeam" in a white, lowercase, sans-serif font, centered within a bright green rounded rectangular box. The background is a gradient of blue and green, with a pattern of small, light-colored dots scattered across it, creating a digital or network-like aesthetic.

veeam