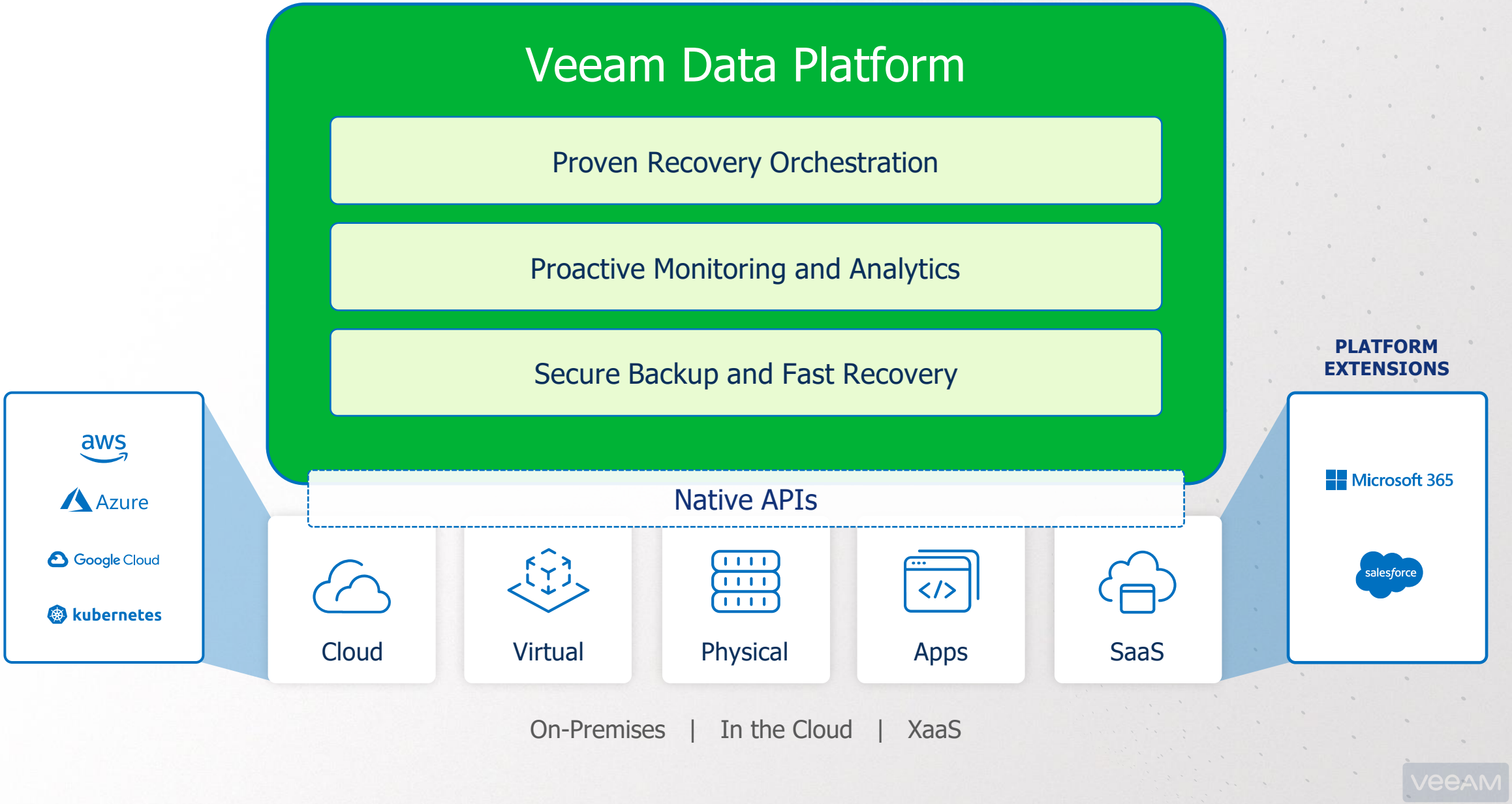
Veeam – So schützen Sie sich vor Ransomware

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
aws
Azure
Google Cloud
kubernetes
PLATFORM EXTENSIONS
Microsoft 365
salesforce
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)

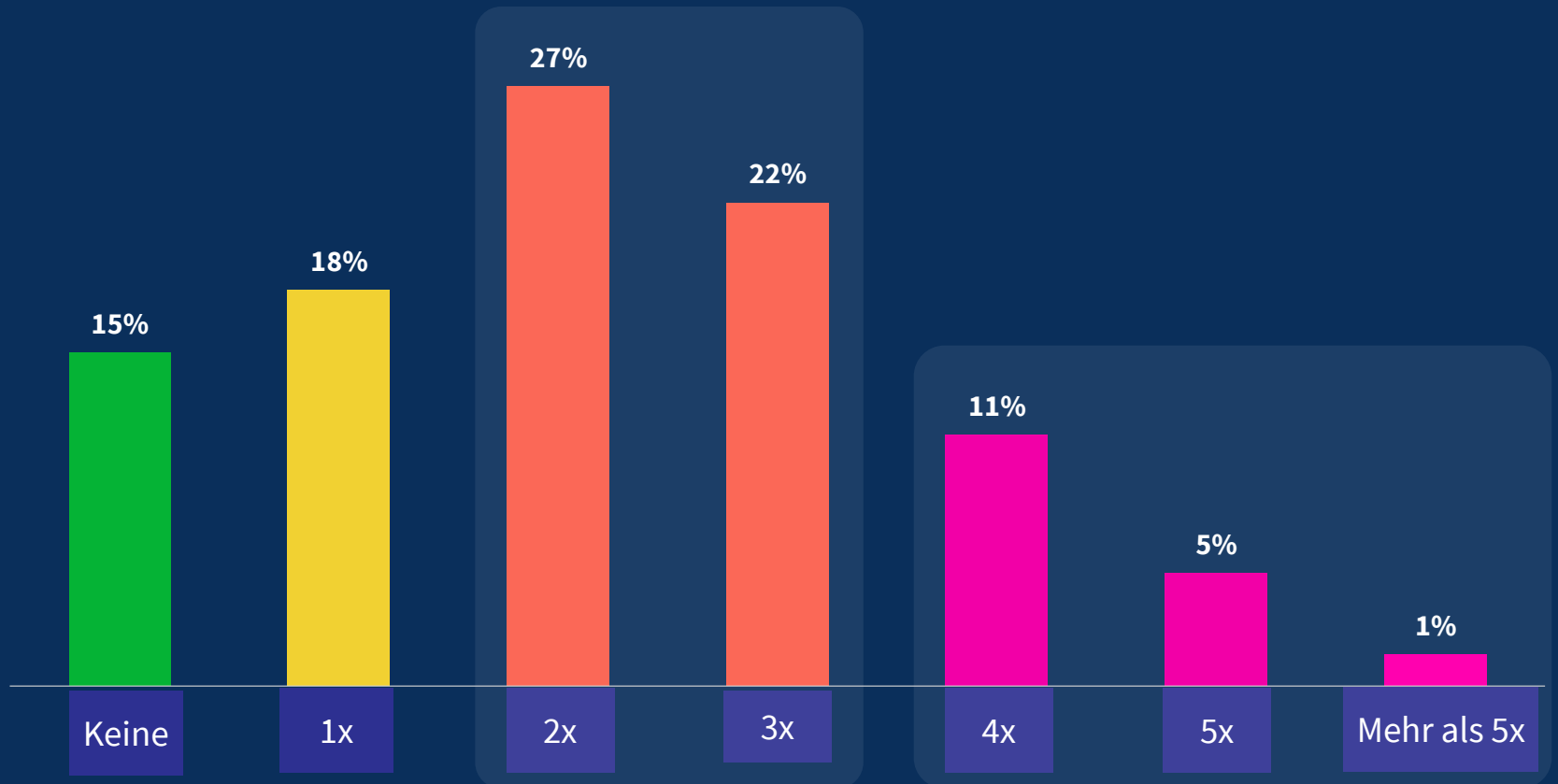
85%

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%**).

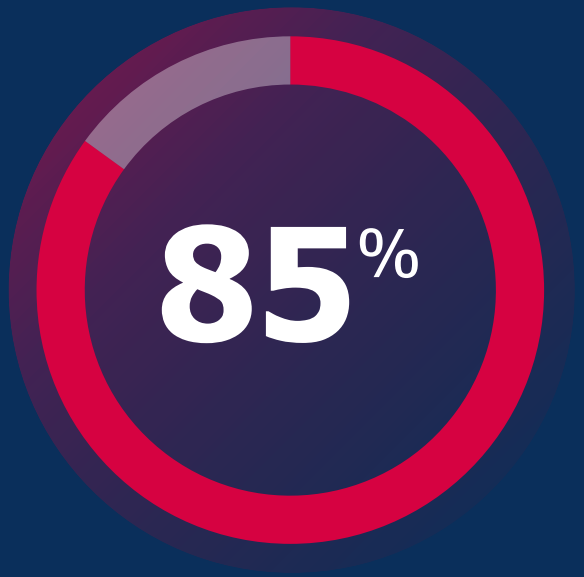
49%

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**

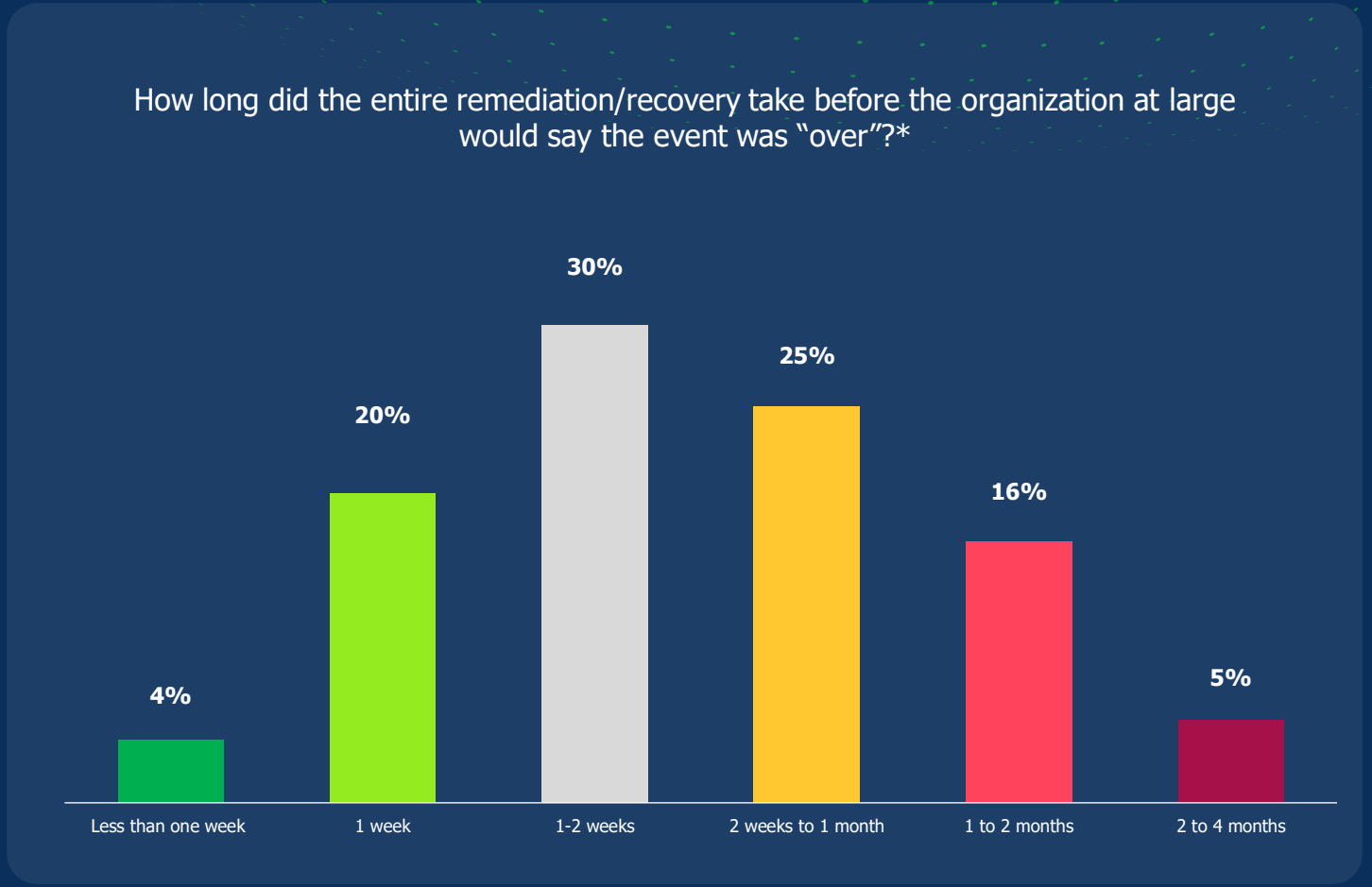
Organizations paid the ransom and never got their data back**

*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



*Source: 2023 **Ransomware Trends Report 2023**

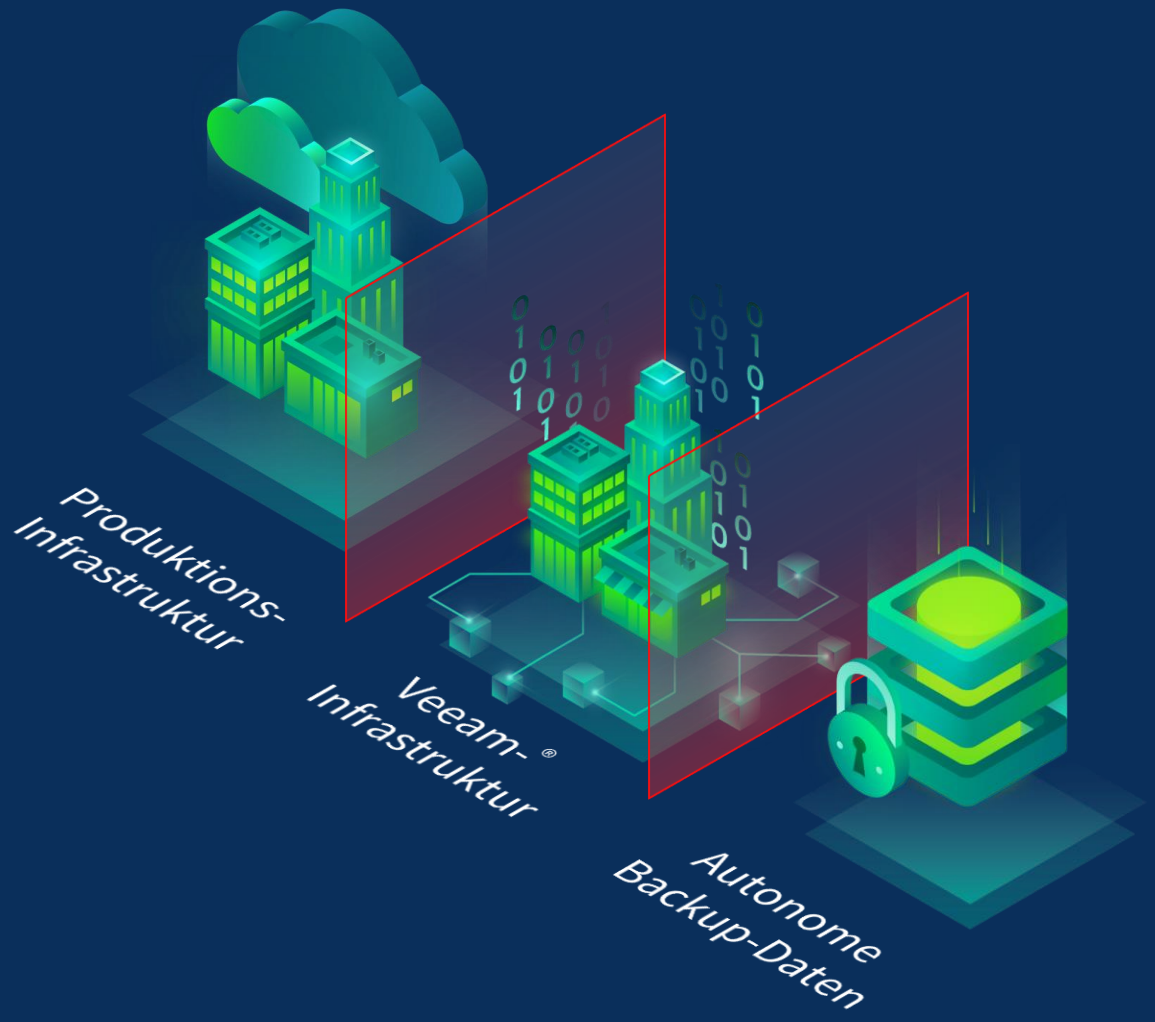
Schutz der Backup-Infrastruktur

Abwehr von Ransomware

Mehrstufiger Schutz

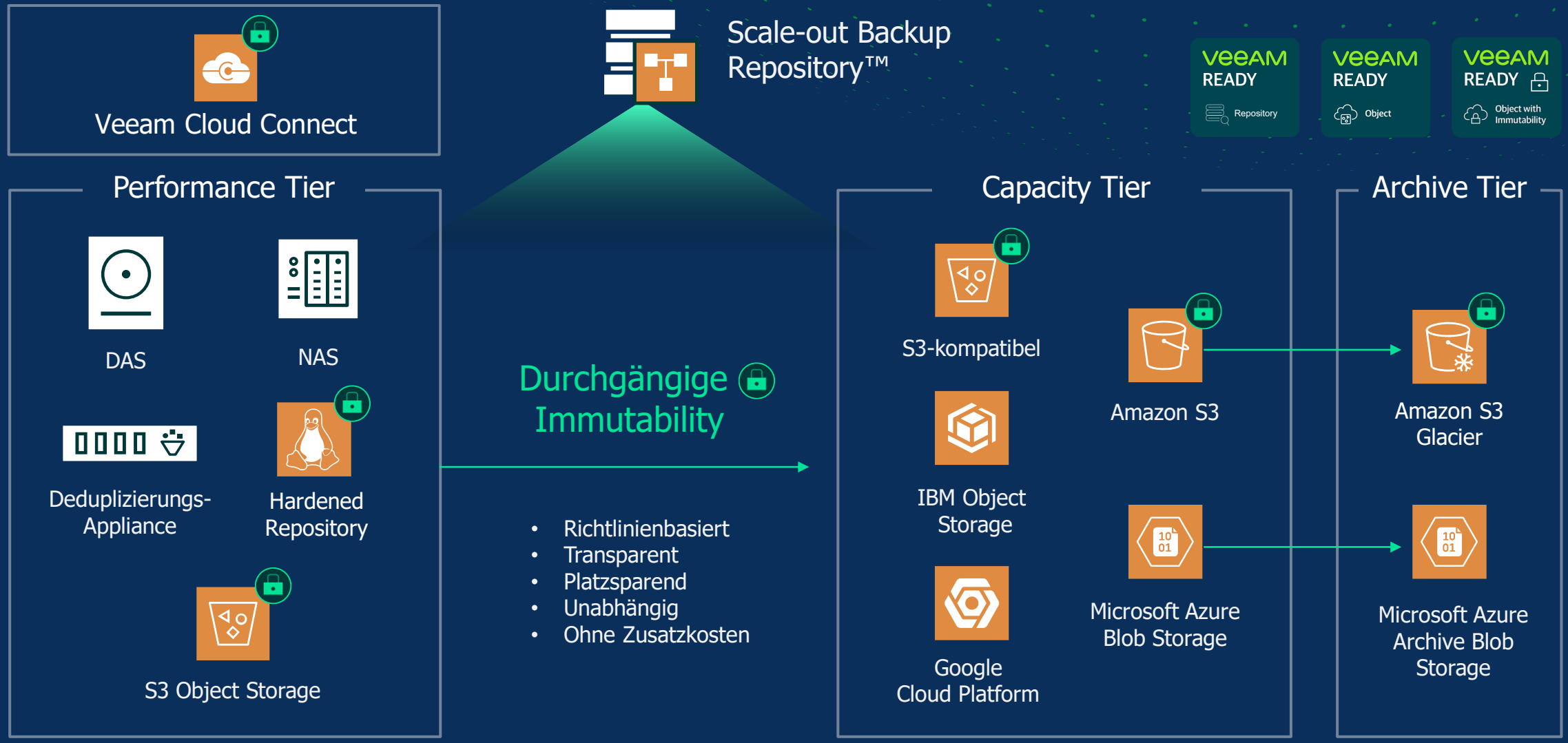
Es gibt keinen Königsweg

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

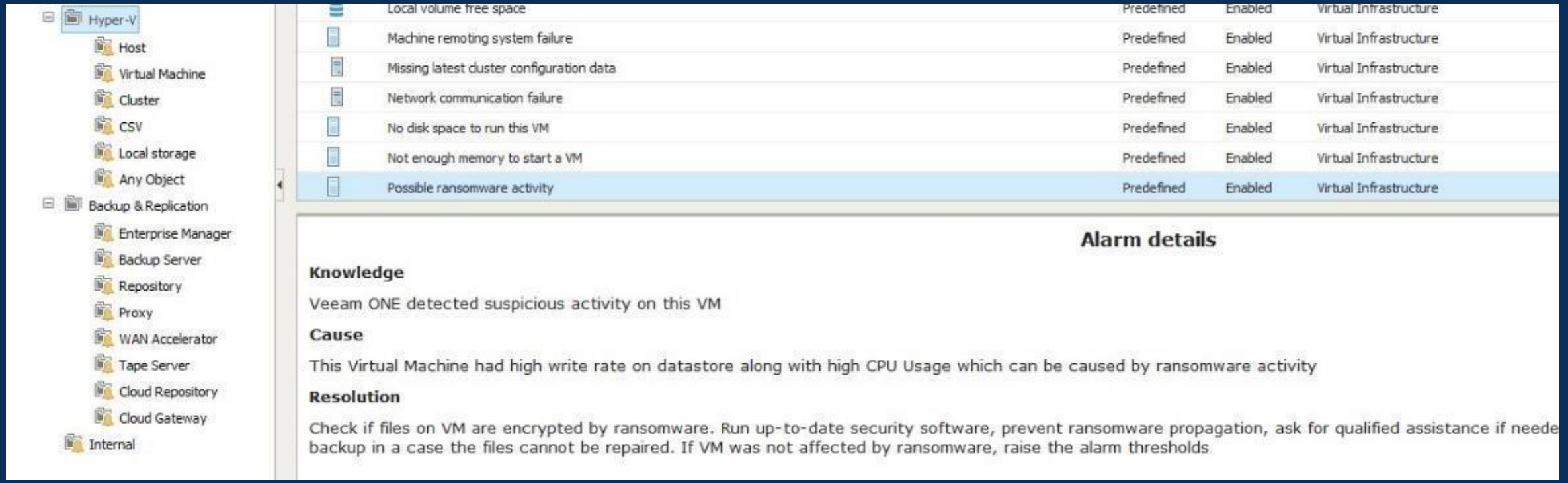
Wieder-herstellung

Sofortige Wiederherstellungen

VEEAM

Ransomware Erkennung

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



Sichere Workload-Tests

Regelmäßiges Testen aller gesicherten Workloads und DR-Szenarien

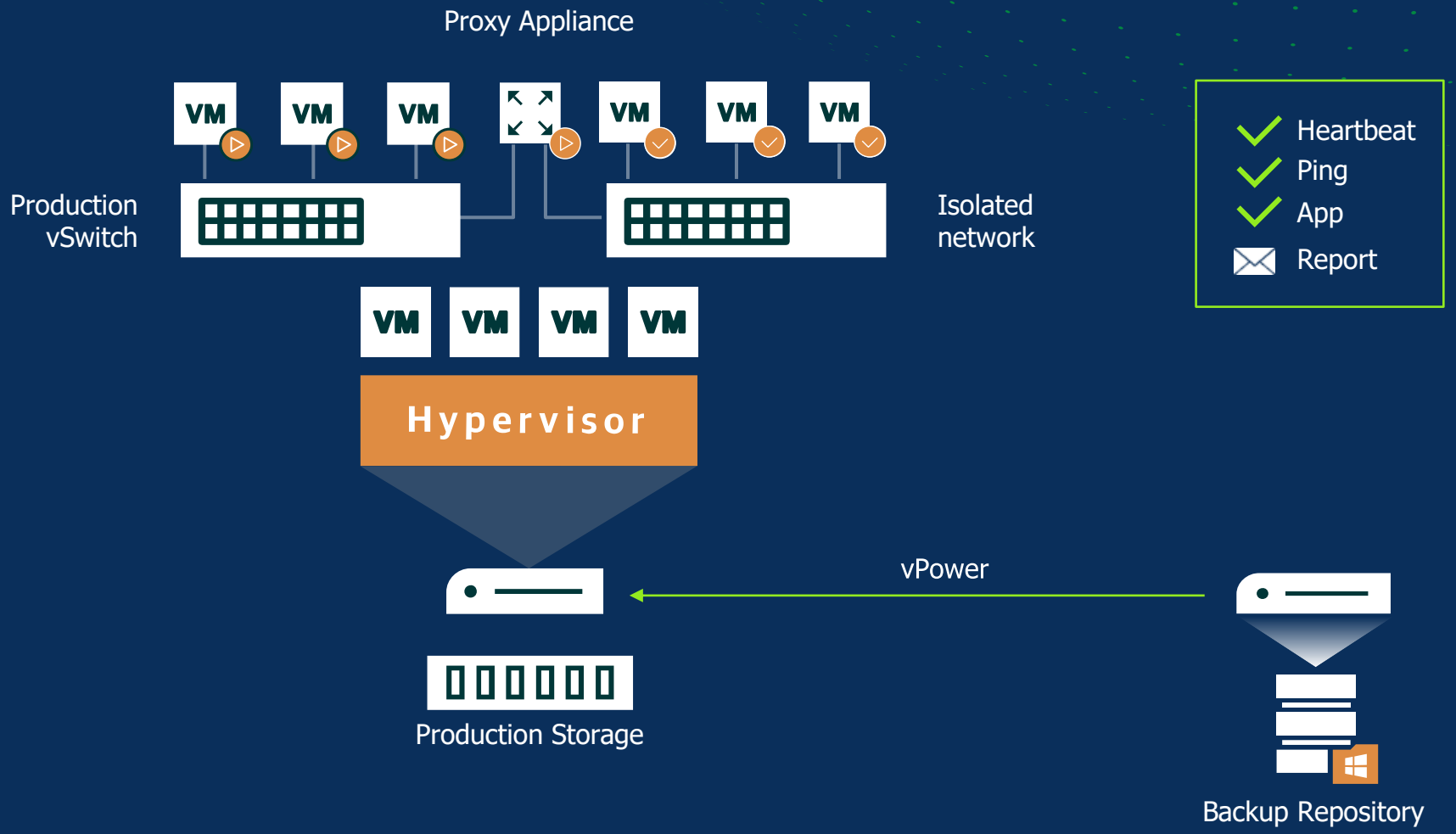
Sind die Backups virenfrei?

- Überprüfung mit aktuellen Virenscanner-Definitionen

~~Never~~ change a running system!

- Regelmäßiges Einspielen von Patches und Updates

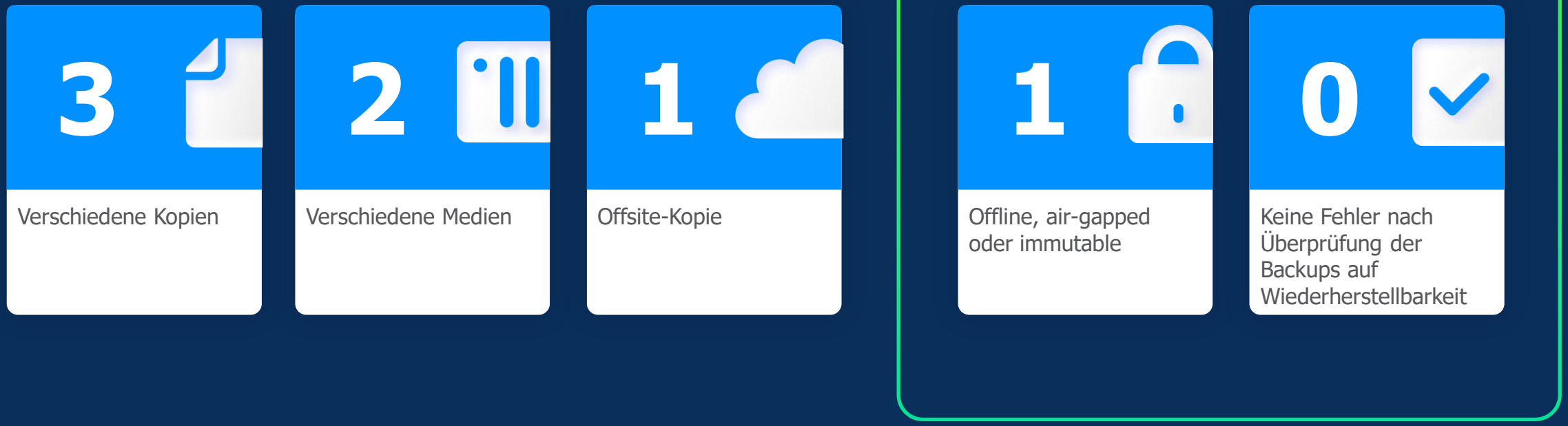
Überprüfung der Backups



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

Vorbereitet sein: die Datenschutz-Postleitzahl



VEEAM

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

VEEAM

Hardened Linux Repository – Überblick

Warum?

Vor Malware geschützte Repositories

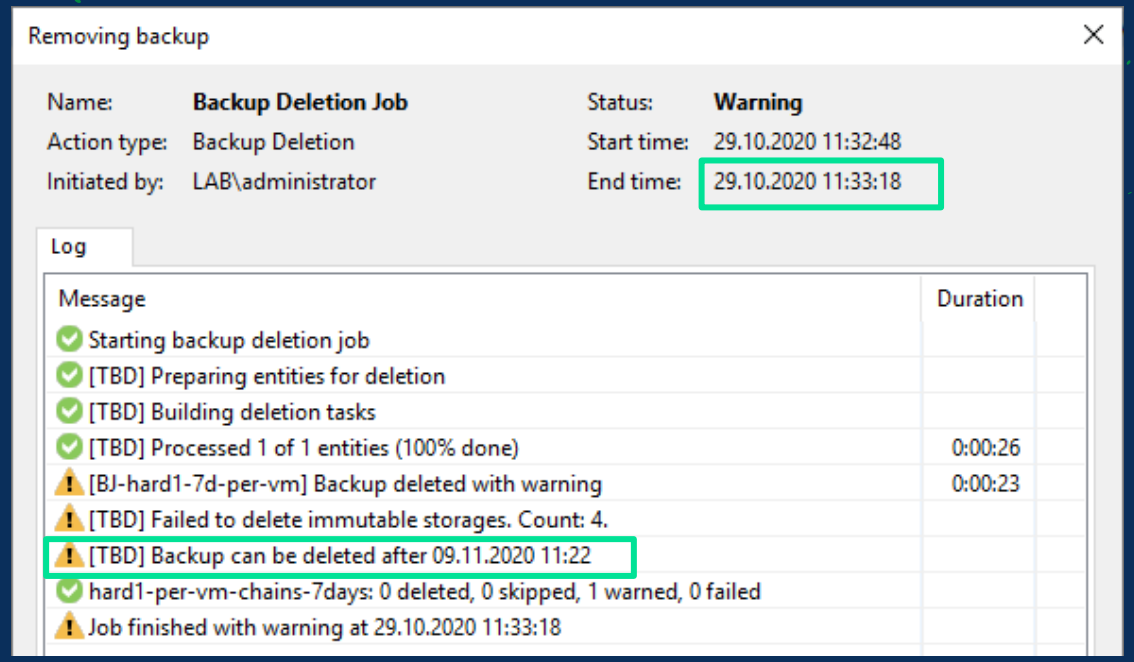
Bei richtiger Konfiguration:
Schutz vor internen Bedrohungen

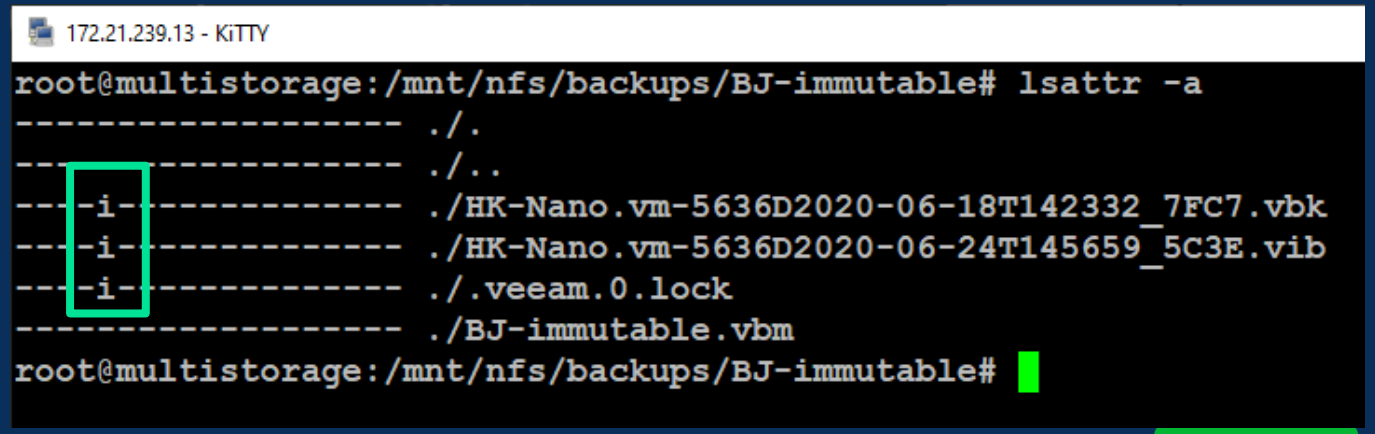
Was?

Backups sind nicht löschbar

Wie?

Verwendung des „immutable"-
Dateisystemattributs unter Linux



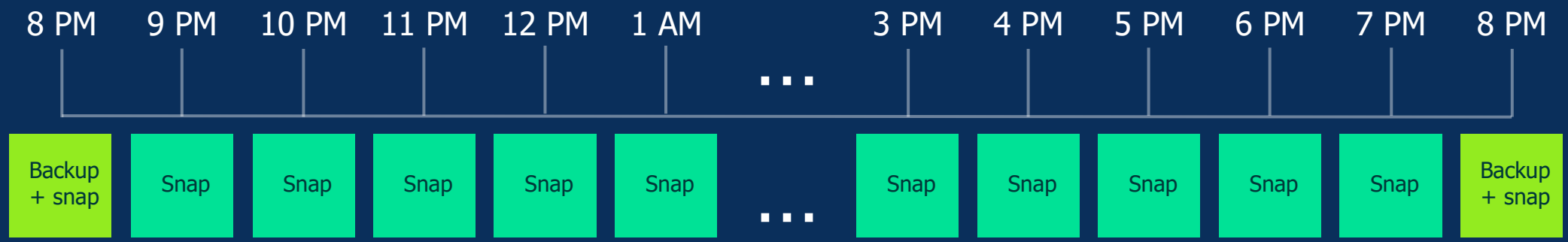


VEEAM

Use of Storage Snapshots for better RTO and RPO

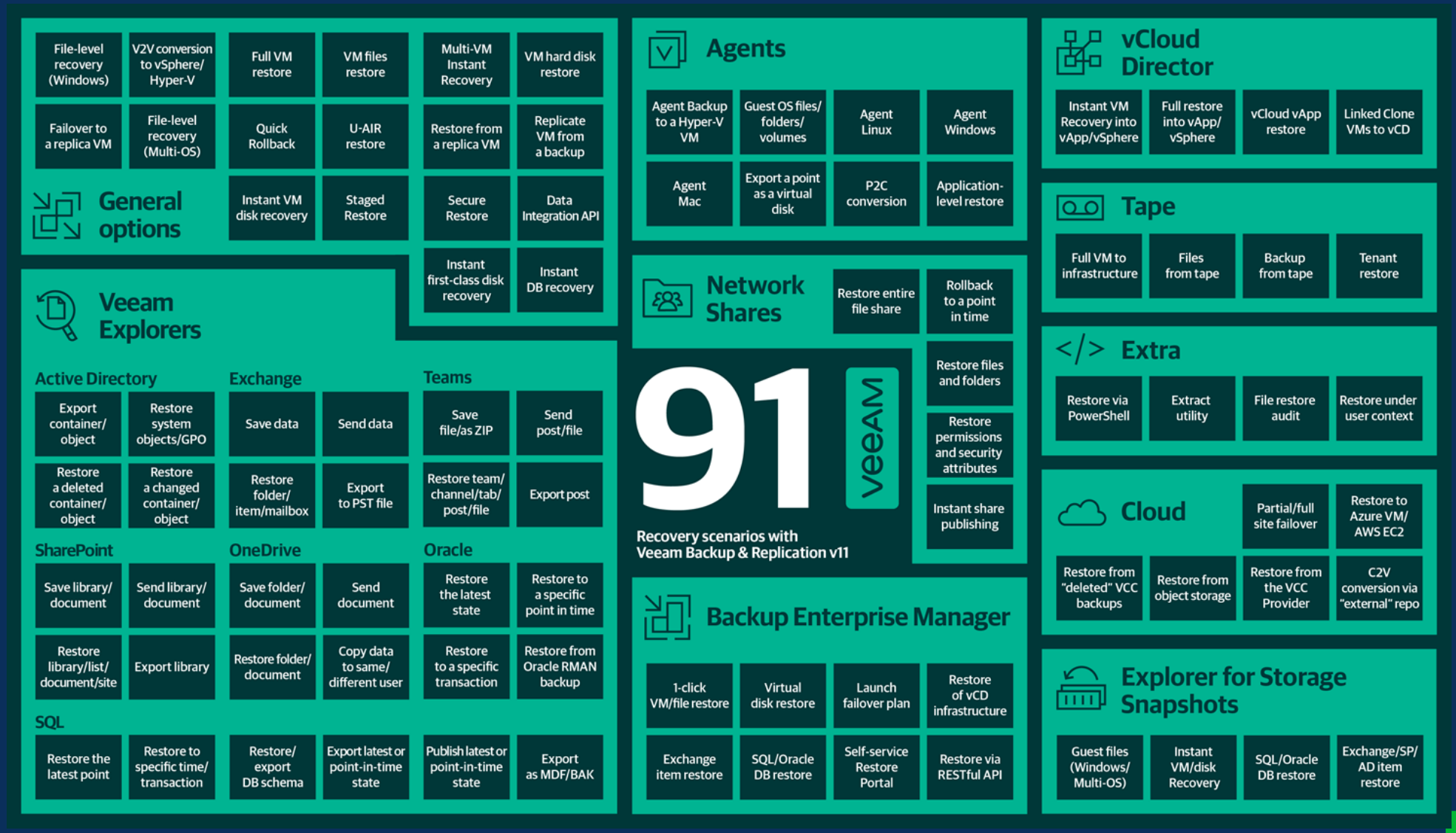
During backup, data transport and consistency processing reduce performance of applications.

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



Wiederherstellung

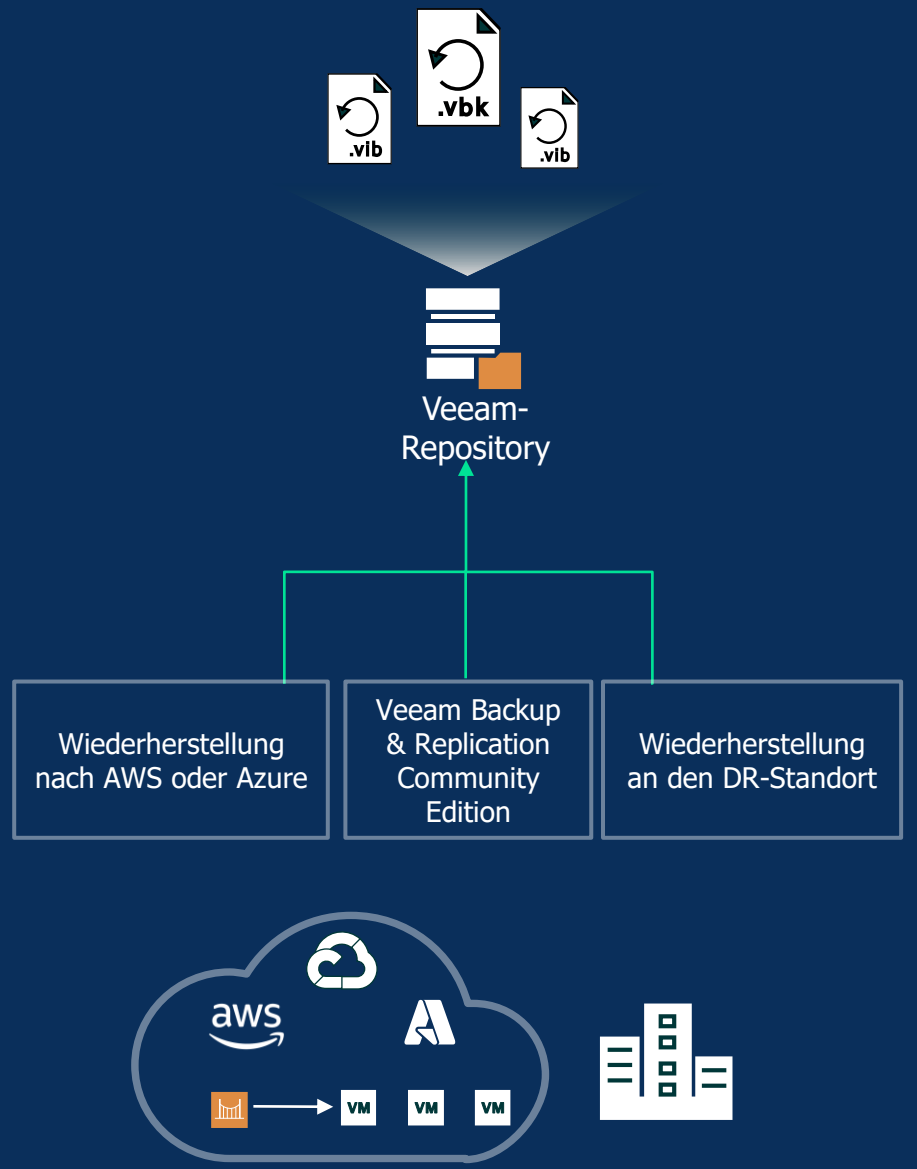
Instant Recovery für alle Workloads



VEEAM

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

Microsoft Windows Defender

ESET NOD32 Smart Security

Symantec Protection Engine

Oder jede andere Antivirensoftware mit CMD-Unterstützung

1. Wiederherstellungspunkt auswählen

Veeam Backup & Replication™

Backup-Repository

Mount Server

2. Backup-Dateien direkt als Laufwerk einhängen

Antivirensoftware mit aktuellen Definitionen installiert

3. Antivirus-Check

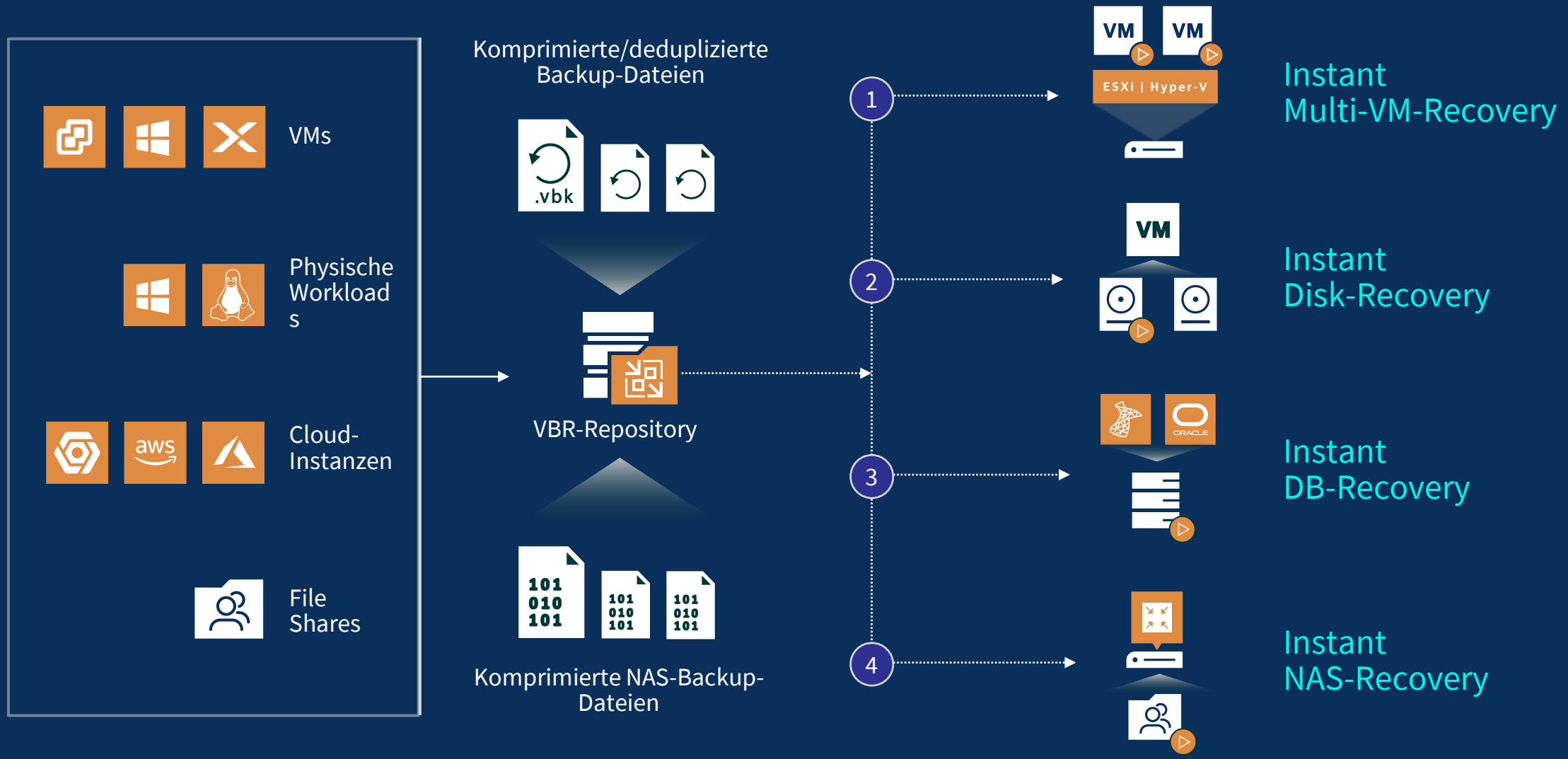
4a. Keine Infektion gefunden; Wiederherstellung fortsetzen

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

4c. Infektion gefunden; Wiederherstellung stoppen

Hypervisor

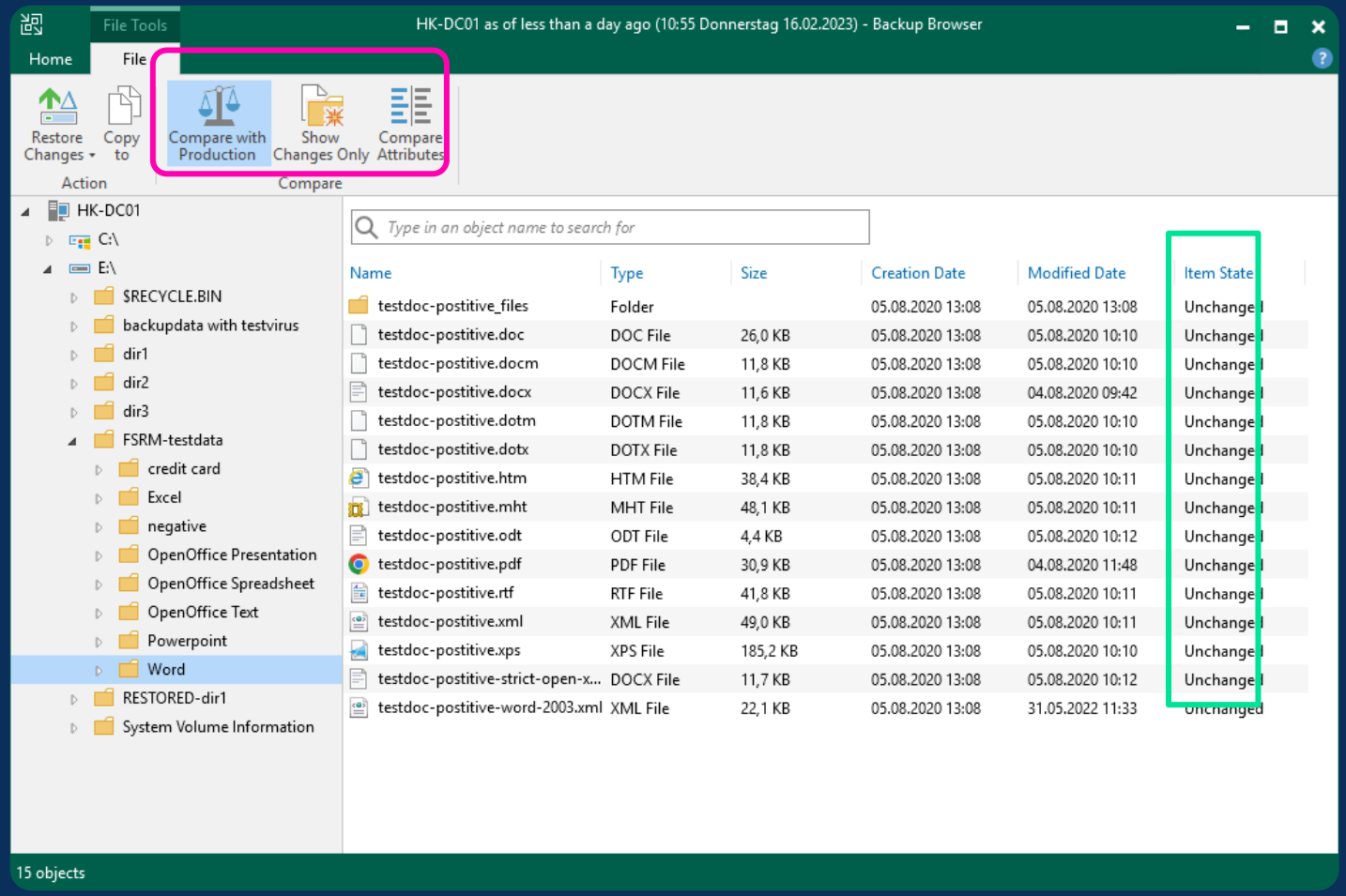
Instant Recovery „at Scale"



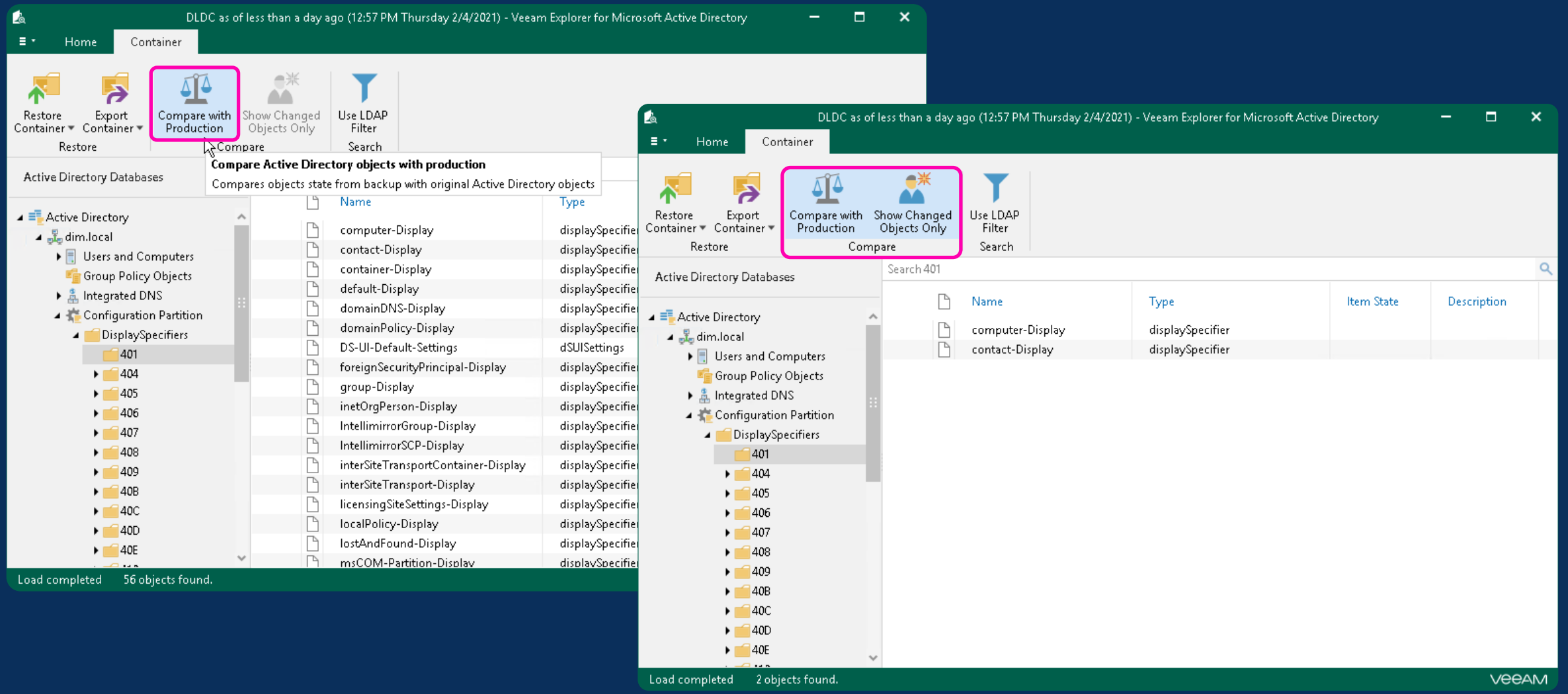
Einfach nur veränderte Dateien wiederherstellen

Windows File Explorer auf Dateiebene im Vergleich zur Produktion

Geänderte Objekte anzeigen, um potenziell verschlüsselte Dateien zu identifizieren



Veeam Explorer™ *for Microsoft Active Directory*



Automatisierung, Test und Dokumentation von DR

Typische DR-Probleme

UNDOKUMENTIERT

UNGETESTET

UNZUVERLÄSSIG

- Komplexität
- Sehr hoher Zeit-/Ressourcenaufwand
- Fehleranfällig

VEEAM

Veeam Disaster Recovery Orchestrator

DYNAMISCHE DOKUMENTE

UNGETESTET

UNZUVERLÄSSIG

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

VEEAM

Veeam Disaster Recovery Orchestrator

DYNAMISCHE DOKUMENTE

AUTOMATISIERTE TESTS

UNZUVERLÄSSIG

- Automatisiert
- Detaillierte Reports
- Keine Beeinträchtigung der produktiven Systeme

Veeam Disaster Recovery Orchestrator

DYNAMISCHE DOKUMENTE

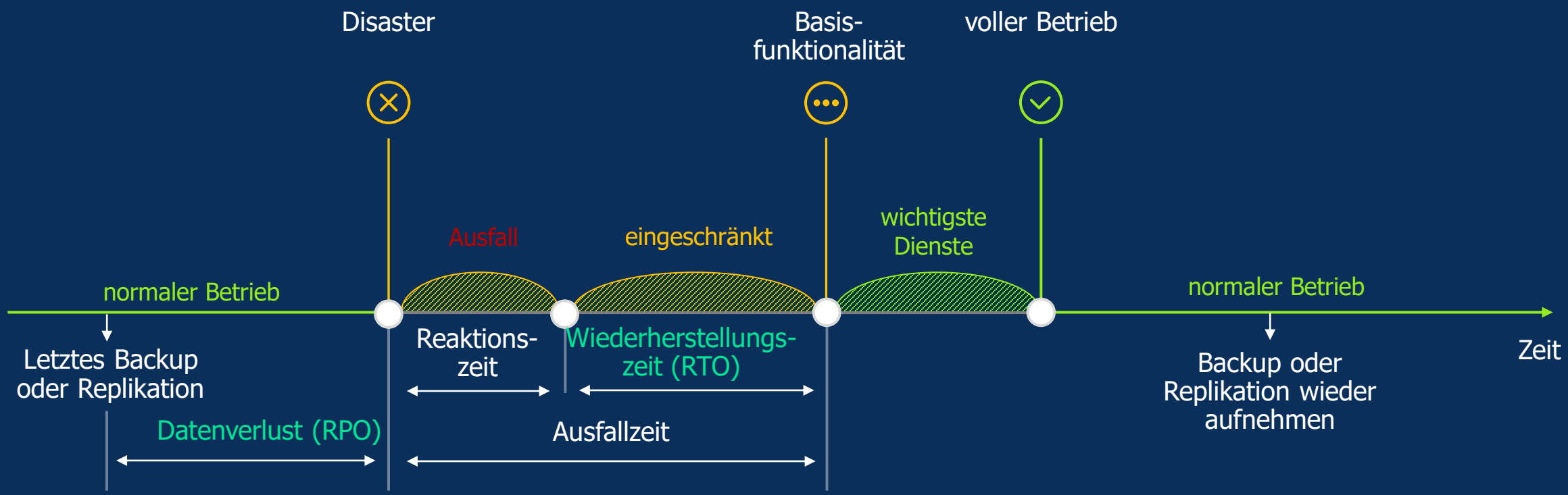
AUTOMATISIERTE TESTS

ZUVERLÄSSIGE WIE-DERHERSTELLUNG

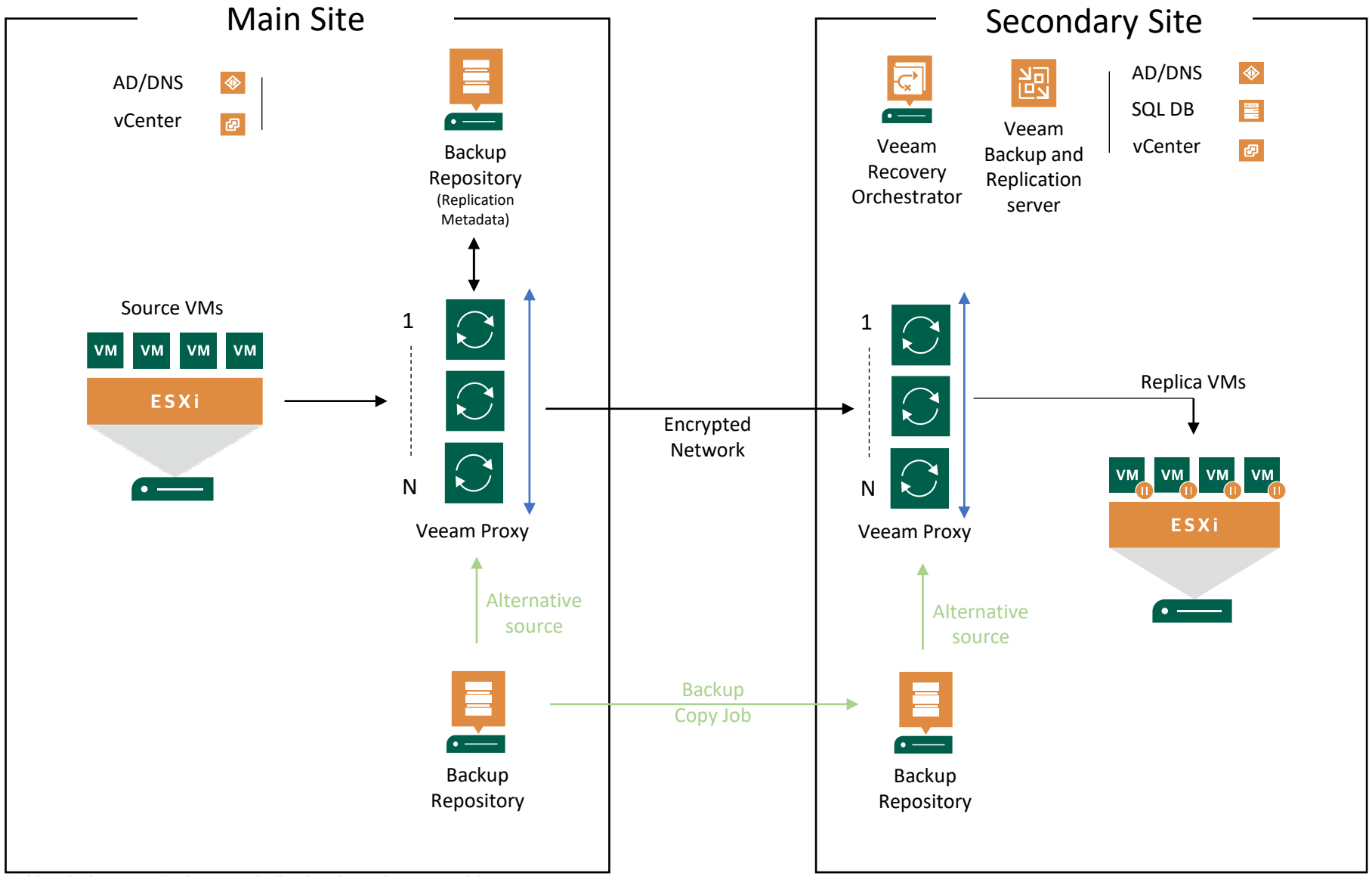
- Automatisiert
- Verifiziert
- Optimiert

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)

Veeam Backup & Replication

Mount Server

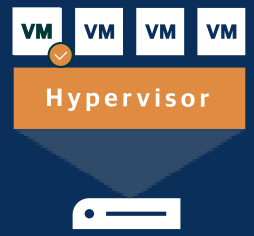
Backup repository

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

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	✓	✓		
Supporting product components	Veeam Backup & Replication	Veeam ONE	Veeam Recovery Orchestrator	

Also Available:

- Veeam Backup & Replication Community Edition

Q&A


VEEAM