

AKDB Forum

*Notfallplan - Ransomware Protection
auch für Ihre Backup Daten!*



Nikolaos Panidis

Enterprise Account Executive Public

Daten Management im Jahr 2022

veeam

Produktion

Komplexe
Infrastruktur

Menschlicher
Fehler

Angriffs-
aktivitäten

Compliance-
Richtlinien

Kurze RTO
Vorgaben

Herausforderungen bei
der Wiederherstellbarkeit

**Wieder-
herstellung**

Exponentielles
Datenwachstum

Sicherheitsrisiken

Manueller Betrieb

Heterogene
Umgebungen

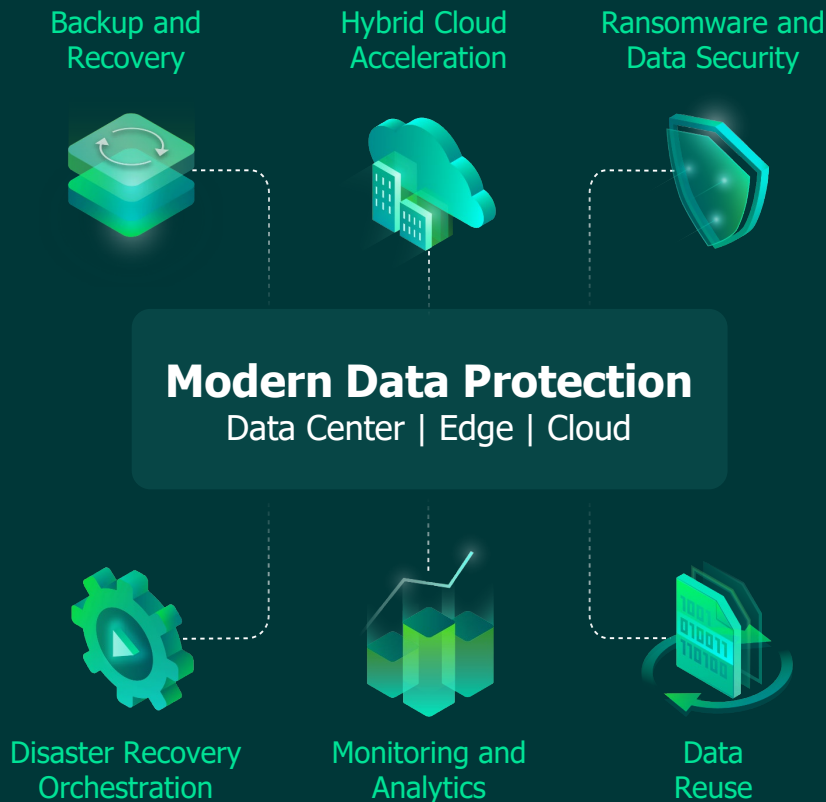
Budgetbeschränkungen

Entwicklung einer
Multi-Cloud-Strategie

Backup

DR-Standort

Anforderungen gehen über Backup hinaus

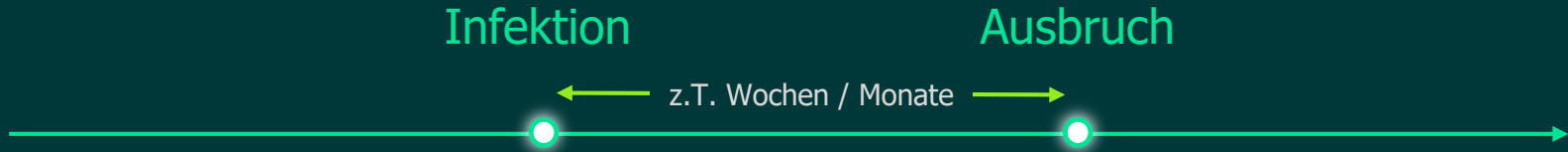


Wie können Sie Ihre Umgebung schützen?





Verlauf einer Ransomware-Attacke

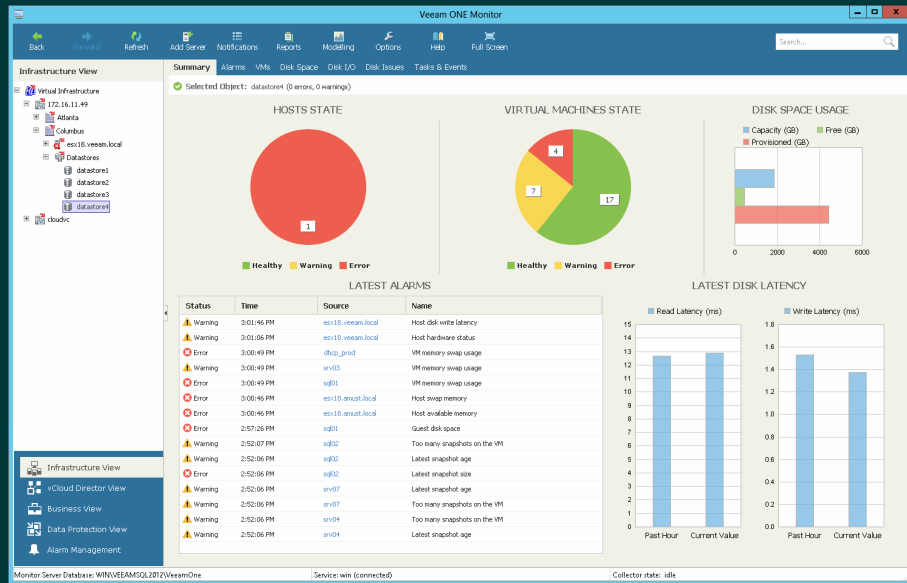


- Proaktives Monitoring
- SureBackup
- 3-2-1 Backup
- Immutability

Echtzeit-Überwachung und -Benachrichtigung rund um die Uhr (24x7) mit Veeam ONE

Für Backups und virtuelle Umgebungen

- Über 200 vordefinierte Benachrichtigungen
- VMs ohne Backup identifizieren
- RPO und RTO Überwachung
- Ransomware-Monitoring möglich
- Schnelle Isolierung und Problemlösung
- Änderungsnachverfolgung



Veeam DataLabs

Wurde entwickelt, um Anwender dabei zu unterstützen, die Verfügbarkeit und Sicherheit zu verbessern, indem Risiken reduziert werden. Schutz vor Malware, Ausrollen von neuen Updates und Patches, DevOps, DevTests und Compliance sind hier nur einige Beispiele.

Features

On-Demand
Sandbox



SureBackup und
SureReplica



Staged Restore

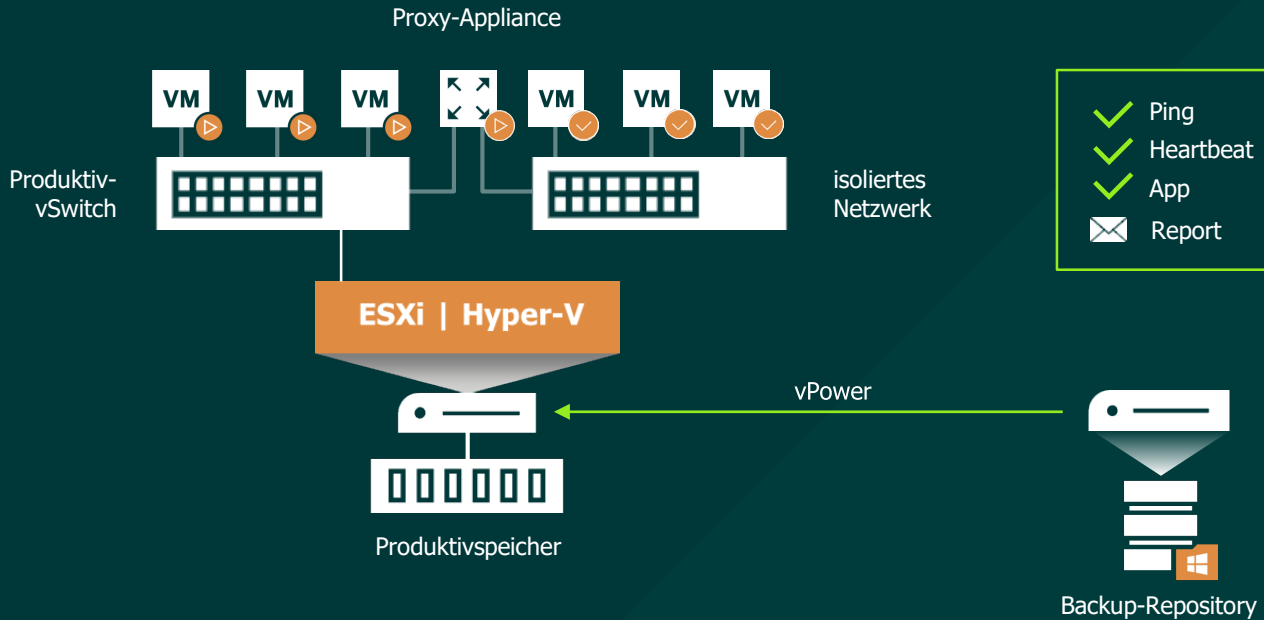


Secure Restore



SureBackup

Regelmäßige, automatisierte Überprüfung Ihrer Backups auf Wiederherstellbarkeit inkl. Ransomware Scan mit aktualisierten Viren Pattern!



Sicherungsstrategie für Datenmanagement

3



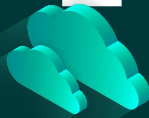
Drei unterschiedliche Datenkopien

2



Zwei unterschiedliche Medien

1



Eine externe Kopie

veeAM

1



Davon ist eine:
offline durch ein
Air-Gap getrennt
oder unveränderlich

0



Keine Fehler nach
der Überprüfung
des automatischen
Backups auf
Wiederherstellbarkeit

Unveränderlichkeit/Immutable



Scale-out Backup
Repository

veeAM
READY

Repository

veeAM
READY

Object

veeAM
READY

Object with
Immutability

Leistungsebene



DAS



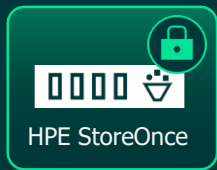
NAS



Abgesichertes
Repository



Objektspeicher



HPE StoreOnce

Durchgängige 
Unveränderlichkeit

- Regelbasiert
- Transparent
- Platzsparend
- Eigenständig
- Ohne Zusatzkosten

Kapazitätsebene



S3-kompatibel



IBM-Objekt-
speicher



Google
Cloud



Amazon S3



Microsoft Azure
Blob Storage



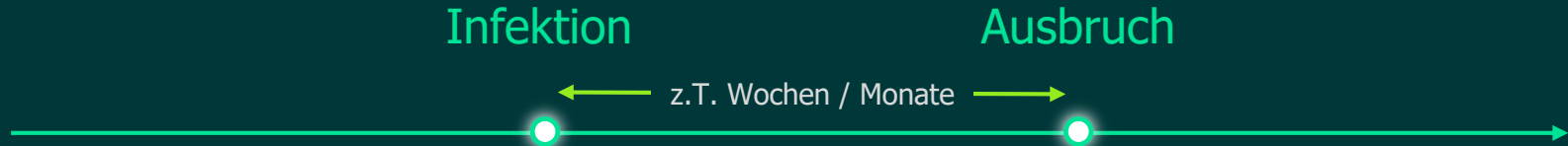
Amazon S3
Glacier



Microsoft Azure
Archive Blob
Storage



Verlauf einer Ransomware-Attacke



- 3-2-1 Backup
- Immutability
- SureBackup

- Veeam ONE
- Data Integration API

Datenanalyse und Scans

Backups und DR testen



Vierteljährliches
Testen von DR
und Backups



Backups sind sinnlos,
wenn sie nicht
funktionieren

Ransomware-Erkennung

Seit bereits 3 Jahren kann Veeam ONE Ransomware-Aktivitäten in produktiven Workloads erkennen.

Veeam ermöglicht die Verwaltung verdächtiger Backup-Daten verschiedener Größen.

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 table of alarms. The alarm 'Possible ransomware activity' is selected and highlighted in blue. Below the table, the 'Alarm details' section provides information about the alarm, including its knowledge, cause, and resolution.

Alarm Name	Severity	Status	Category
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.

Possible Ransomware Activity Alarm

- Veeam One überwacht auch CPU-Last, Datastore-Schreibrate und Netzwerkauslastung
- Funktioniert für VMs
- Dies wird für die Erkennung von Ransomware genutzt werden
- Kopieren und anpassen für VMs, die so ein Verhalten im Regelbetrieb haben

The screenshot displays the 'Alarm Settings' interface in Veeam One. On the left, a sidebar lists navigation options: General, Rules (selected), Assignment, Notifications, Actions, Suppress, and Knowledge Base. The main area shows three configured rules, each with a checkbox to enable or disable it.

Rule 1 (AND):

- Rule type: Usage
- Counter: CPU Usage (%)
- Condition: Above
- Warning: 78.0 %
- Error: 82.5 %
- Time period: 5 min
- Aggregation: Avg

Rule 2 (AND):

- Rule type: Usage
- Counter: Datastore Write Rate (KBps)
- Condition: Above
- Warning: 45.0 MB/s
- Error: 60.0 MB/s
- Time period: 5 min
- Aggregation: Avg

Rule 3 (OR):

- Rule type: Usage
- Counter: Network Transmit Rate (K...
- Condition: Above
- Warning: 40.0 MB/s
- Error: 60.0 MB/s
- Time period: 5 min
- Aggregation: Avg

Suspicious Incremental Backup Size Alarm

- Analysiert die letzten drei inkrementellen Backup-Läufe
- Alarm wird getriggert bei 150% (Warning) bzw. 200% (Error)
- Alarm funktioniert sowohl für VM Backups als auch für Hardware Agenten
- Alarm kann angepasst und kopiert werden

The screenshot shows the 'Alarm Settings' window in Veeam Backup & Replication. The 'Rules' tab is selected. There are two rules listed, both for 'Incremental backup size'.

Rule	Rule type	Job type	Detection type	Condition	Warning (%)	Error (%)
1	Incremental backup size	Any	Relative	Above	150.0	200.0
2	Incremental backup size	Any	Relative	Below	80.0	70.0

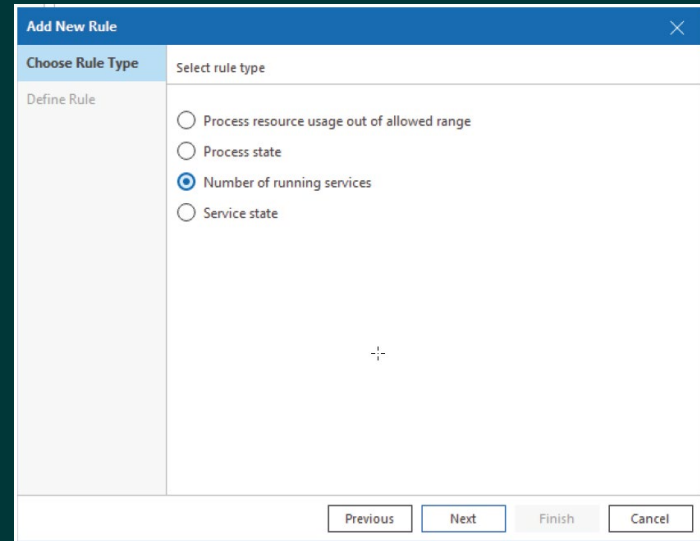
Additional settings for the first rule include: Analysis depth: 3, Job name: *, and an option to suppress the restore point following a job scope change (unchecked). The second rule is currently selected and highlighted in blue.

By default rules work with the OR logic.

Buttons: Add..., Move up, Move down, Link..., Unlink, Remove, Defaults, Save, Cancel.

Anzahl laufender Prozesse monitoren

- Anzahl der Prozesse monitoren
- Erkennen ungewollter Prozesse/Dienste
- Auslösen eines Alarm
- „Gegenmaßnahmen“ einleiten
 - VM schnell sichern
 - Skript ausführen (VM runterfahren?)



Data Integration API – Anwendungsbeispiele

Um Drittanbietersoftware den Zugriff auf Inhalte in Veeam-Backups zu ermöglichen

- Sicherheitsanalysen
- Datenforensik
- e-Discovery (erweiterte Suchfunktionen)
- Klassifizierung von Daten
- Data-Mining (Datensammlung)



API



Verlauf einer Ransomware-Attacke

Infektion

Ausbruch

← z.T. Wochen / Monate →

- 3-2-1 Backup
- Immutability
- SureBackup

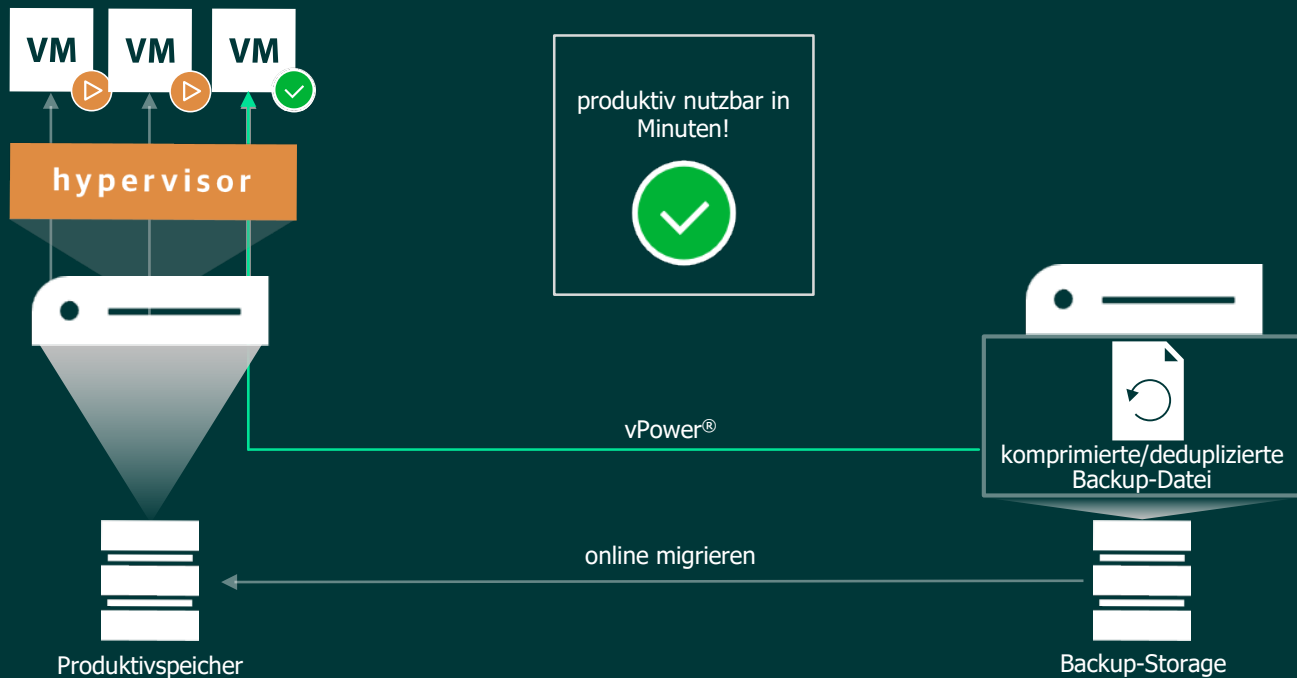
- Veeam ONE
- Data Integration API

- Schnelle Wiederherstellung
- Secure Restore
- DataLabs Forensics

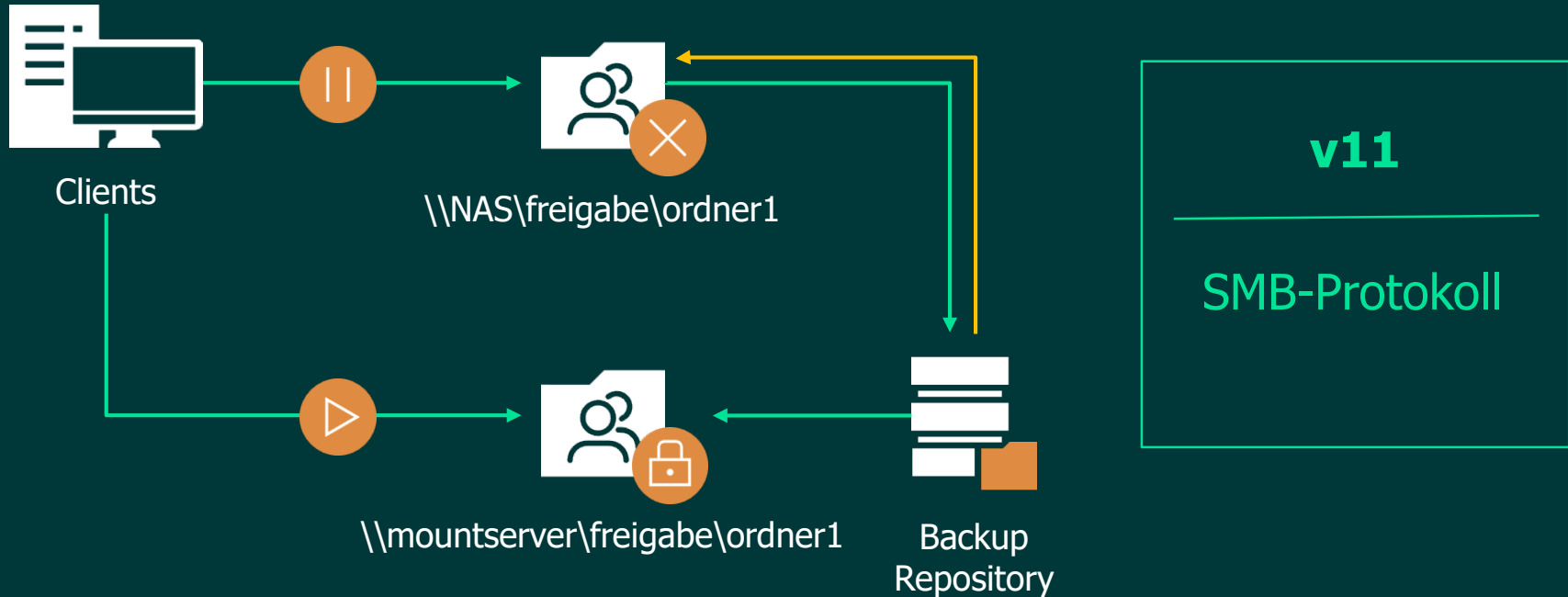


Schnelle Wiederherstellung

Instant VM Recovery von jedem Backup



Instant File Recovery für SMB / NAS Filer

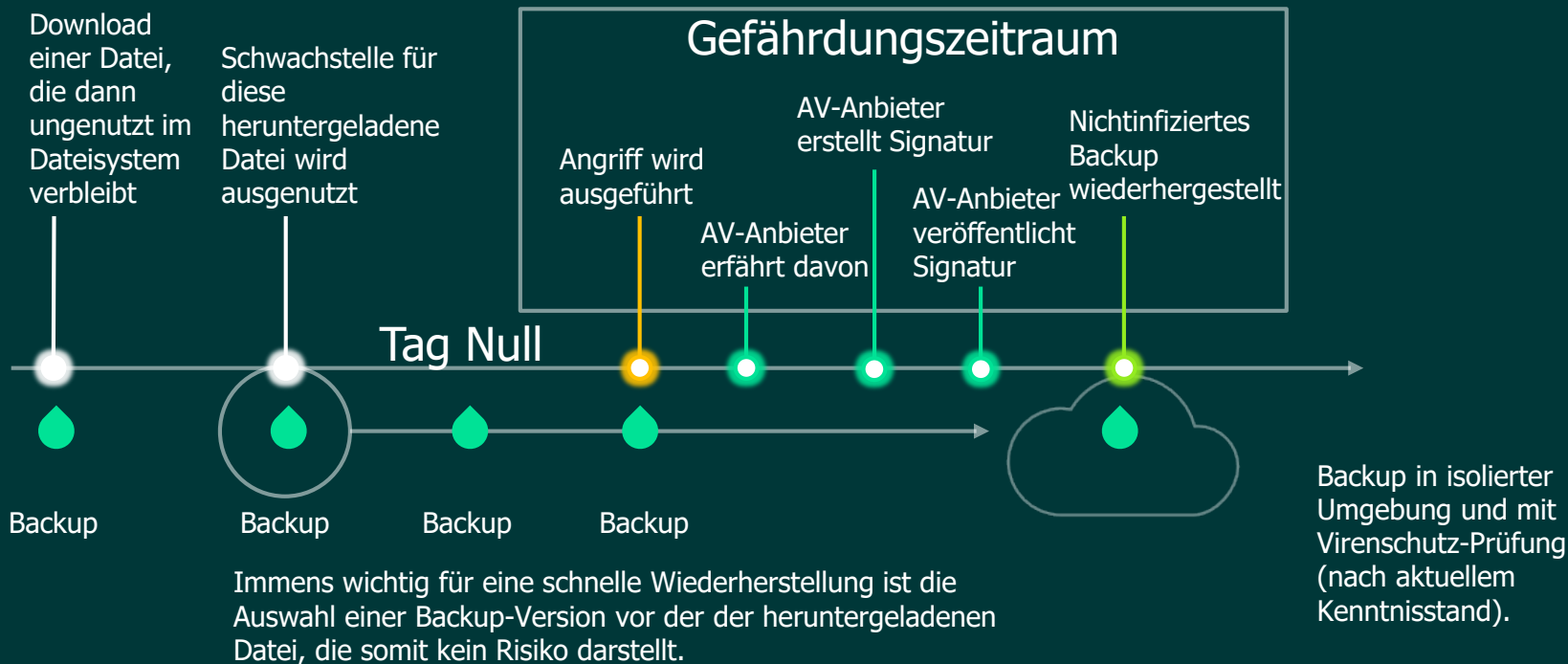




Sichere Wiederherstellung

Sichere Wiederherstellung

Vermeidet erneuten Kontakt mit Schwachstelle, durch die Zero-Day-Lücken ausgenutzt werden können



Sichere Wiederherstellung

Restoring VM

Name: **vmwin110** Status: **In progress (0%)**

Restore type: Full VM Restore Start time: 09.06.2022 12:07:11

Initiated by: VBRSRV60\Administrator [Cancel restore task](#)

Statistics Reason Parameters Log

Message

- ✓ [Windows Defender] Antivirus resource has been acquired
- ▶ Performing antivirus scan for [vmwin110]
- ✓ Mount operation had some errors, not all disks may have been scanned for malware.
- ✓ [Volume{fc15954b-b58d-4236-8148-9337635dff15}] No threats detected. Exit code: 0

Task Manager

File Options View

Processes Performance Users Details Services

Name Status

- ▼ Antimalware Service Executable
 - Microsoft Defender Antivirus Service
- VeeamAgent
- VeeamAgent

Restoring VM

Name: **vmwin110**

Status: **In progress (0%)**

Restore type: Full VM Restore

Start time: 09.06.2022 12:07:11

Initiated by: VBRSRV60\Administrator

[Cancel restore task](#)

Statistics Reason Parameters Log

Message

- | Message | Durat... |
|---|----------|
| ✓ Antivirus scan has been completed for [vmwin110]: Scanned volumes: [C:], [Volume{fc15954b-b58d-4236-8148-9337635dff15}] No threats detected. Exit code: 0 | 0:06:53 |
| ✓ Mount operation had some errors, not all disks may have been scanned for malware. | |
| ✓ [Volume{fc15954b-b58d-4236-8148-9337635dff15}] No threats detected. Exit code: 0 | |
| ✓ [C:] No threats detected. Exit code: 0 | |
| ✓ Starting restore job | |
| ✓ Restoring from SOBR02 | |
| ✓ Queued for processing at 09.06.2022 12:14:21 | |
| ▶ Processing vmwin110 | 0:00:35 |
| ✓ Required backup infrastructure resources have been assigned | |
| ✓ Locking required backup files | 0:00:02 |

Zusammengefasst: Veeam Ransomware Protection

Datensicherheit

Secure Backup/Secure Restore

Data locality

Immutable storage

Data tagging

Integration API

SLA validation



Business view

Monitoring and alerting

DataLabs™

Item-level recovery

Instant recovery

Orchestration



Echte und unabhängige Immutability ermöglicht Daten vor Ransomware zu schützen



Secure Backup, um Workloads und Daten zu schützen und durch automatisierte Tests und Verifizierung sicherzustellen, dass keine Fehler auftreten



Instant Recovery, wodurch die Wiederherstellung günstiger ist als die Zahlung eines Lösegelds



Orchestrierung zur vollständigen Automatisierung und Dokumentation komplexer Workflows, unterbrechungsfreier Wiederherstellungstests

Vielen Dank!

The Veeam logo is displayed within a bright green rectangular box. The word "veeam" is written in a lowercase, white, sans-serif font.

Ihr Ansprechpartner:

Herr Nikolaos Panidis

Enterprise Account Executive Public

Mobil: +49 (0) 170 – 3161454

Tel: +49 (0) 89 – 8393 1456

e-Mail: Nikolaos.Panidis@veeam.com