AKDB Forum

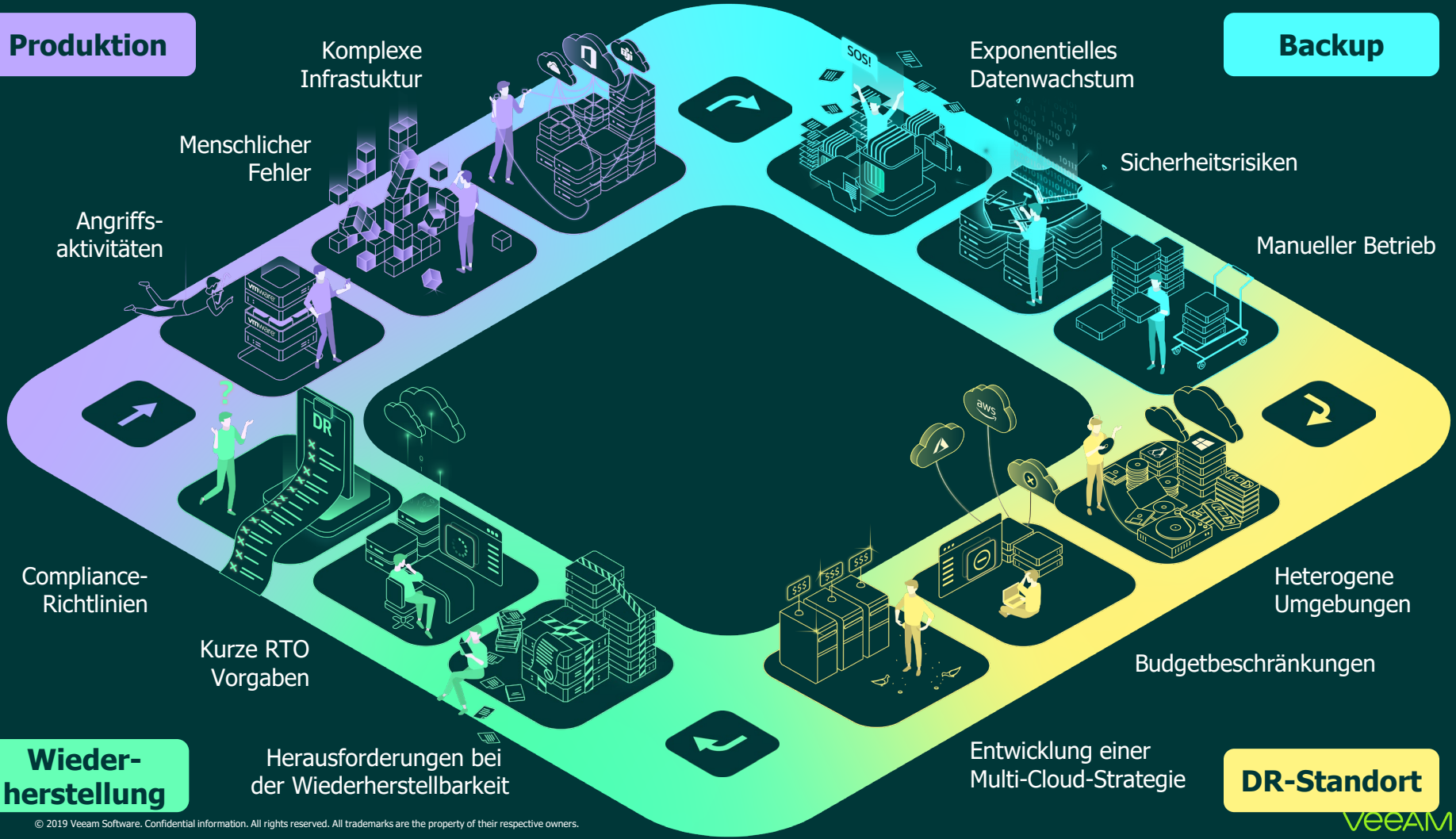
Notfallplan - Ransomware Protection auch für Ihre Backup Daten!

Nikolaos Panidis
Enterprise Account Executive Public

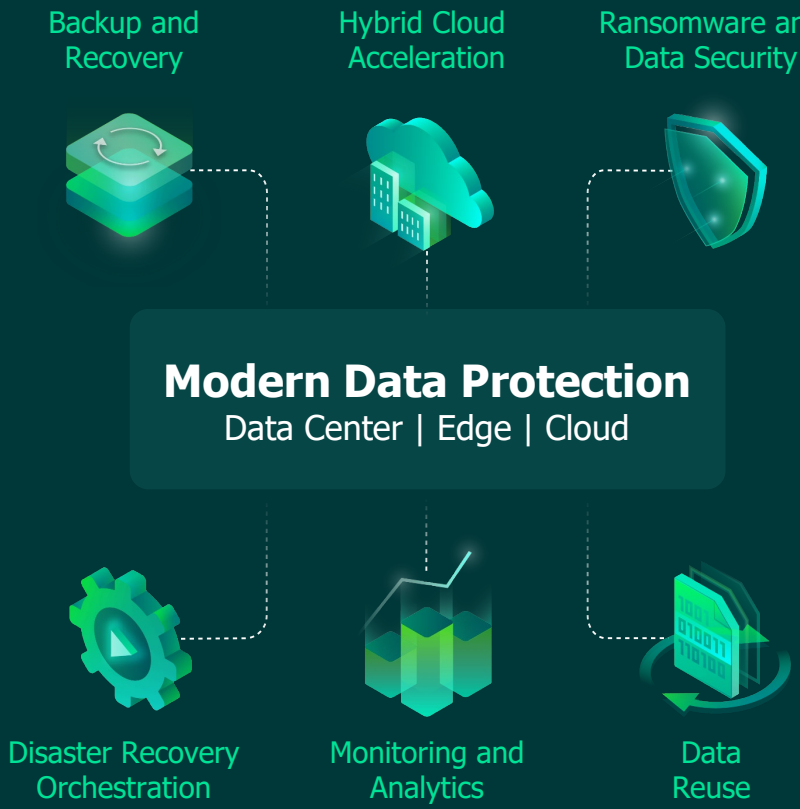
20. Oktober 2022

Daten Management im Jahr 2022

VEEAM



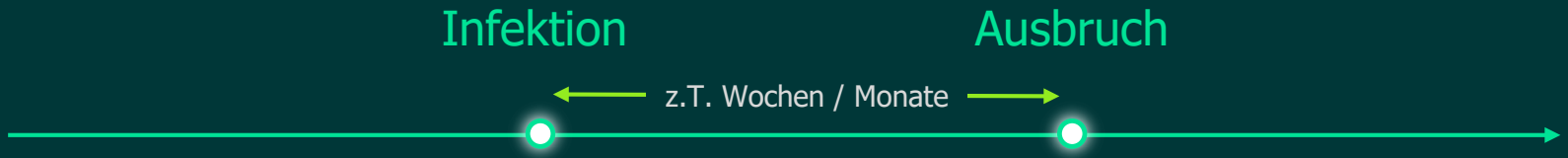
Anforderungen gehen über Backup hinaus



VEEAM

Wie können Sie Ihre Umgebung schützen?

Verlauf einer Ransomware-Attacke

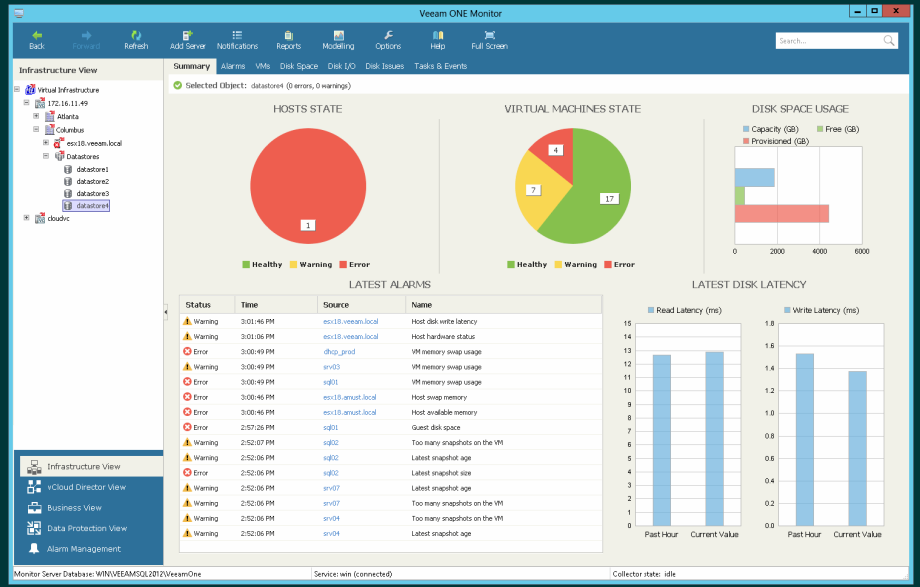


- Proaktives Monitoring
- SureBackup
- 3-2-1 Backup
- Immutability

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

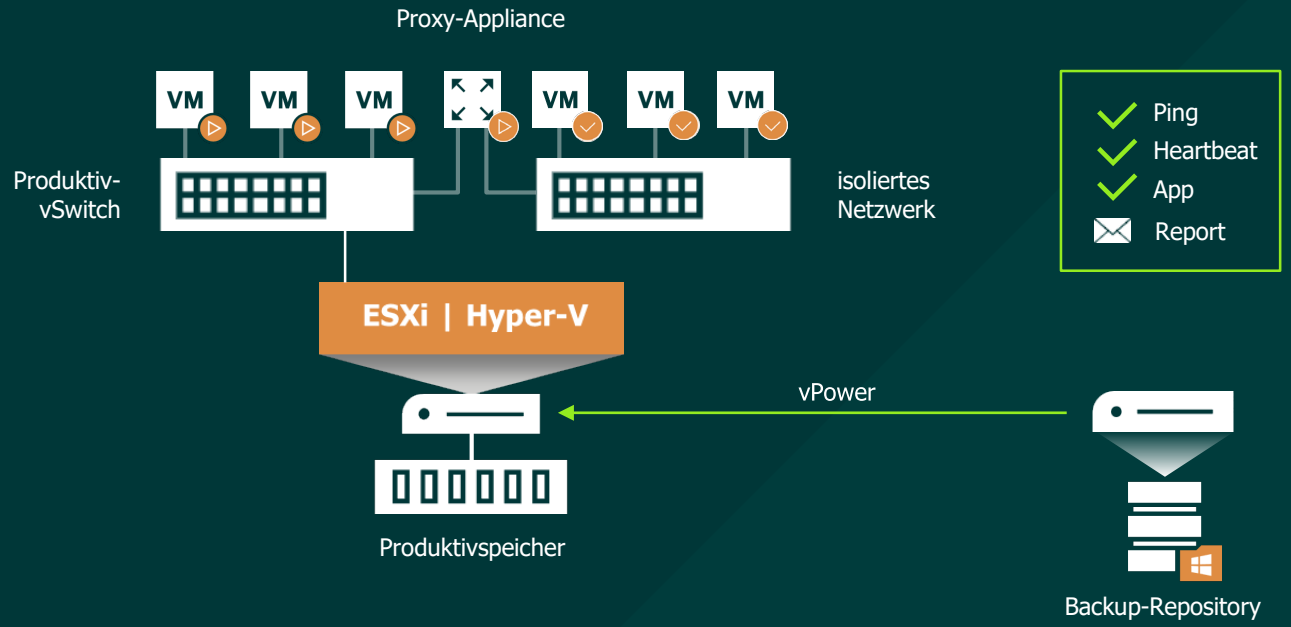
SureBackup und SureReplica

Staged Restore

Secure Restore

SureBackup

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



VEEAM

Sicherungsstrategie für Datenmanagement

VEEAM

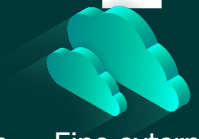
3

Drei unterschiedliche Datenkopien

2

Zwei unterschiedliche Medien

1



Eine externe Kopie

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

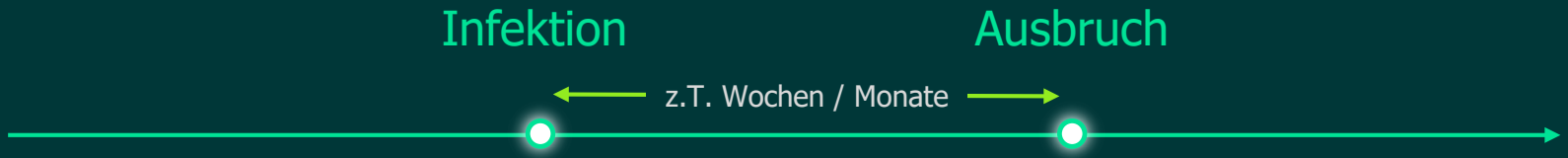
Archivebene

Amazon S3 Glacier

Microsoft Azure Archive Blob Storage

VEEAM

Verlauf einer Ransomware-Attacke



- 3-2-1 Backup
- Immutability
- SureBackup

- Veeam ONE
- Data Integration API

Datenanalyse und Scans

Backups und DR testen

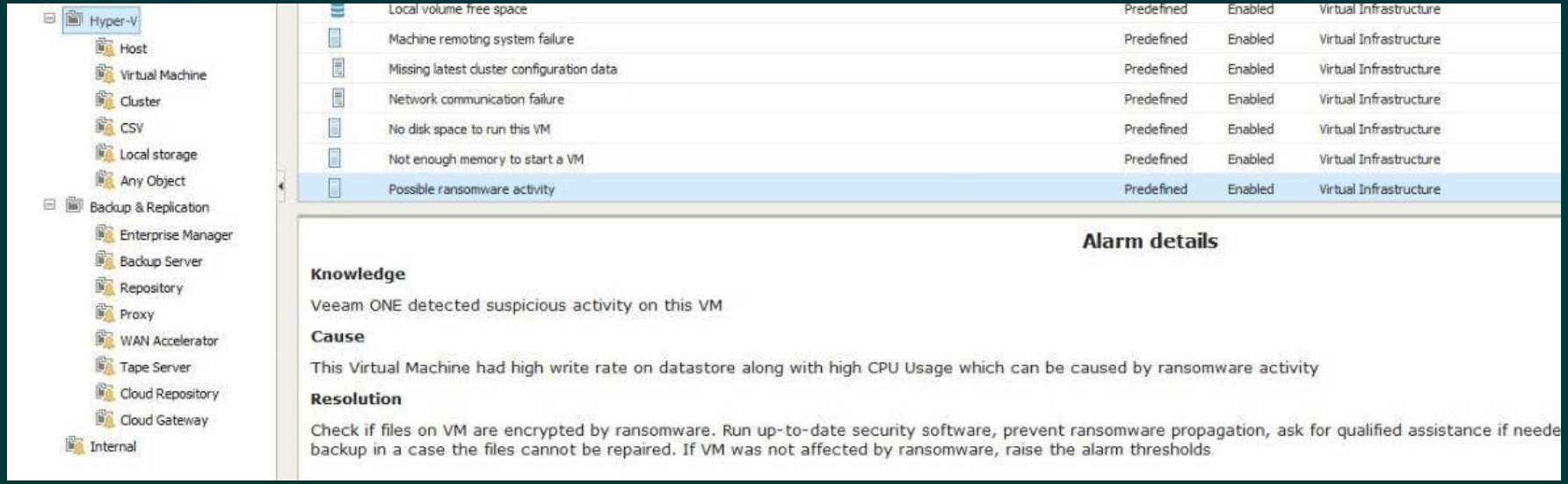
Vierteljährliches Testen von DR und Backups

Backups sind sinnlos, wenn sie nicht funktionieren

Ransomware-Erkennung

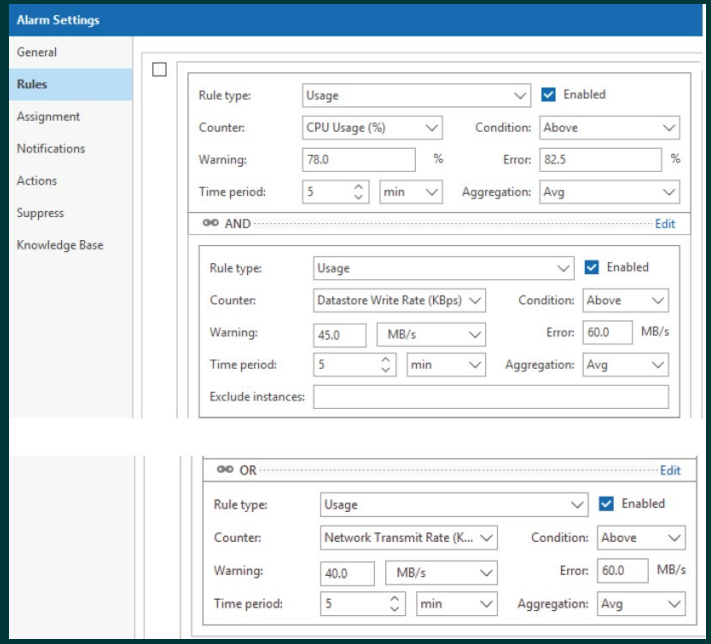
Seit bereits 3 Jahren kann Veeam ONE Ransomware-Aktivitäten in produktiven Workloads erkennen.

Veeam ermöglicht die Verwaltung verdächtiger Backup-Daten verschiedener Größen.



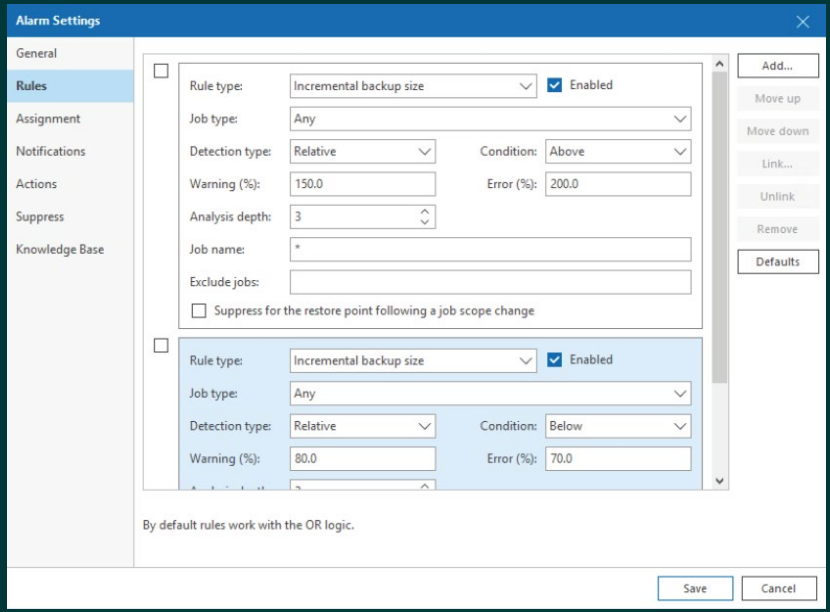
Possible Ransomware Activity Alarm

- 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



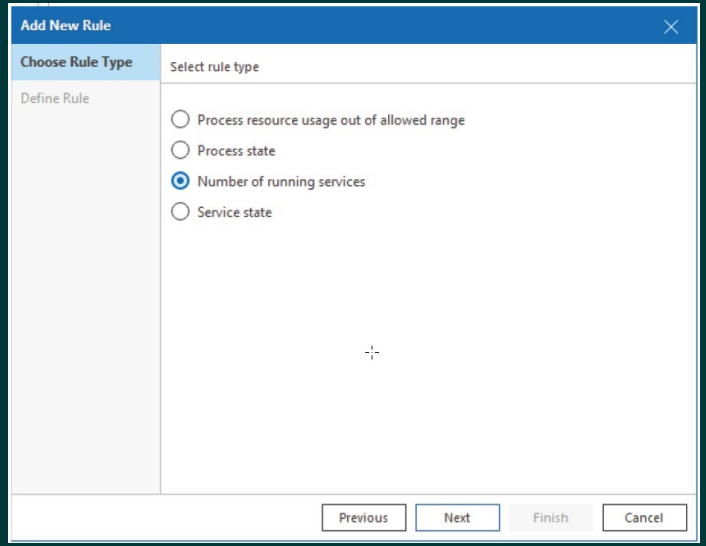
Suspicious Incremental Backup Size Alarm

- 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



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

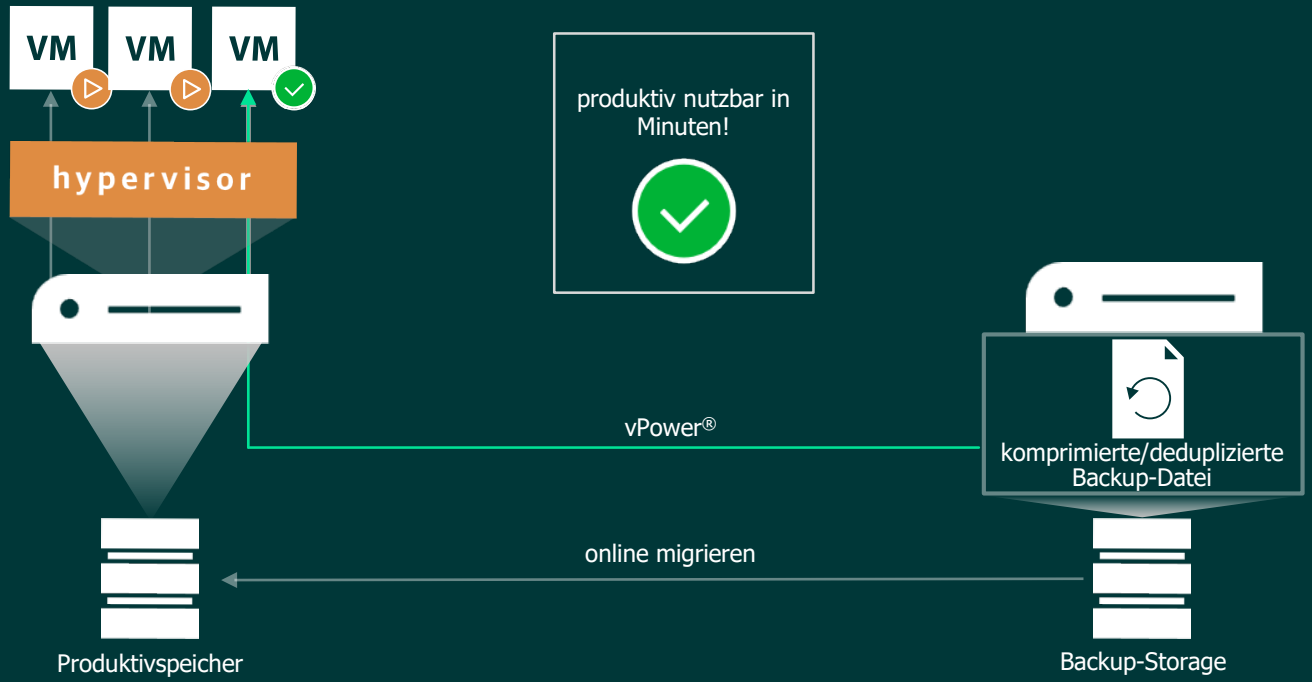
- 3-2-1 Backup
- Immutability
- SureBackup

- Veeam ONE
- Data Integration API

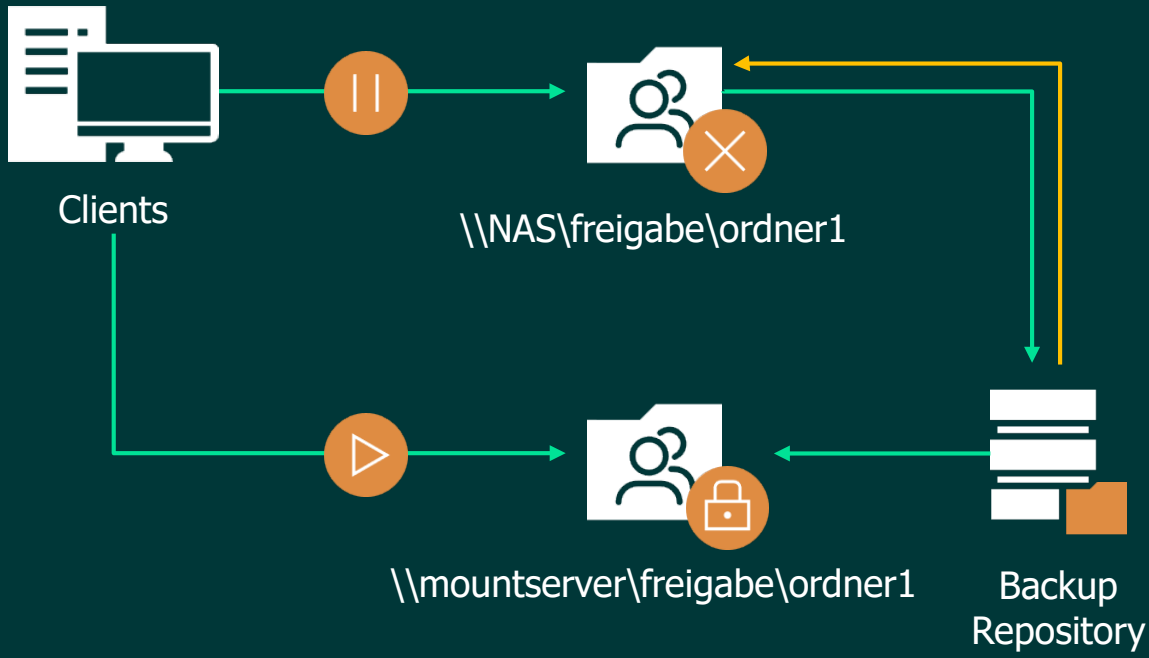
- Schnelle Wiederherstellung
- Secure Restore
- DataLabs Forensics

Schnelle Wiederherstellung

Instant VM Recovery von jedem Backup



Instant File Recovery für SMB / NAS Filer



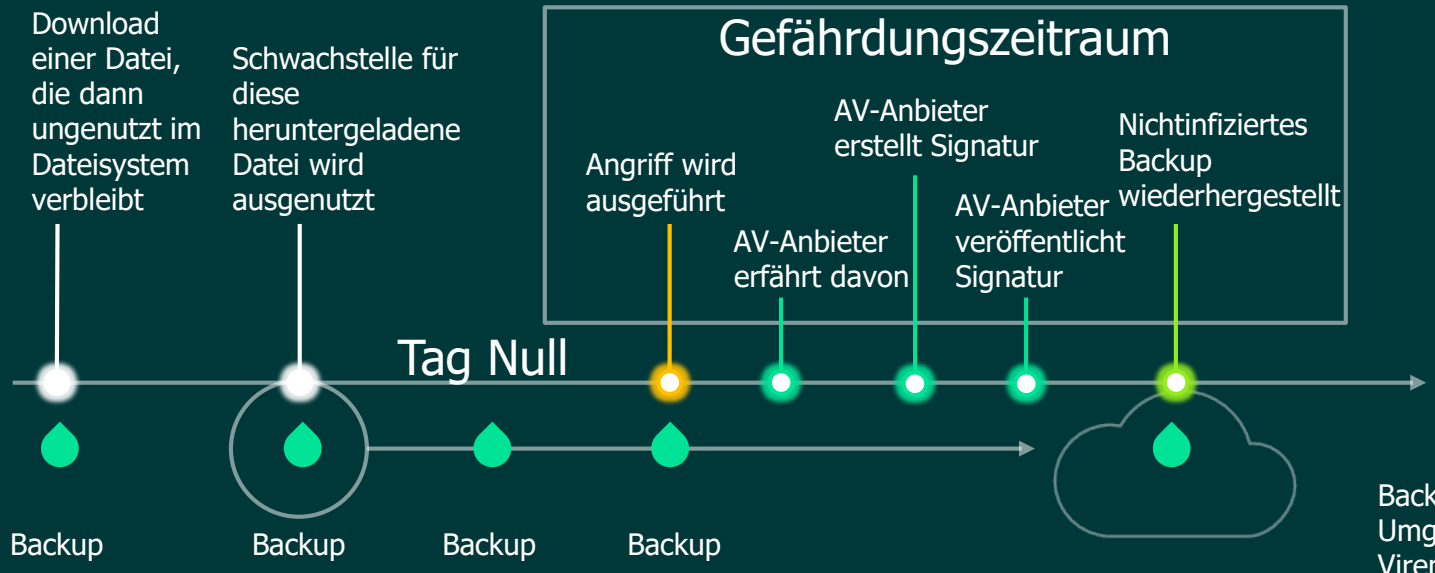
v11

SMB-Protokoll

Sichere Wiederherstellung

Sichere Wiederherstellung

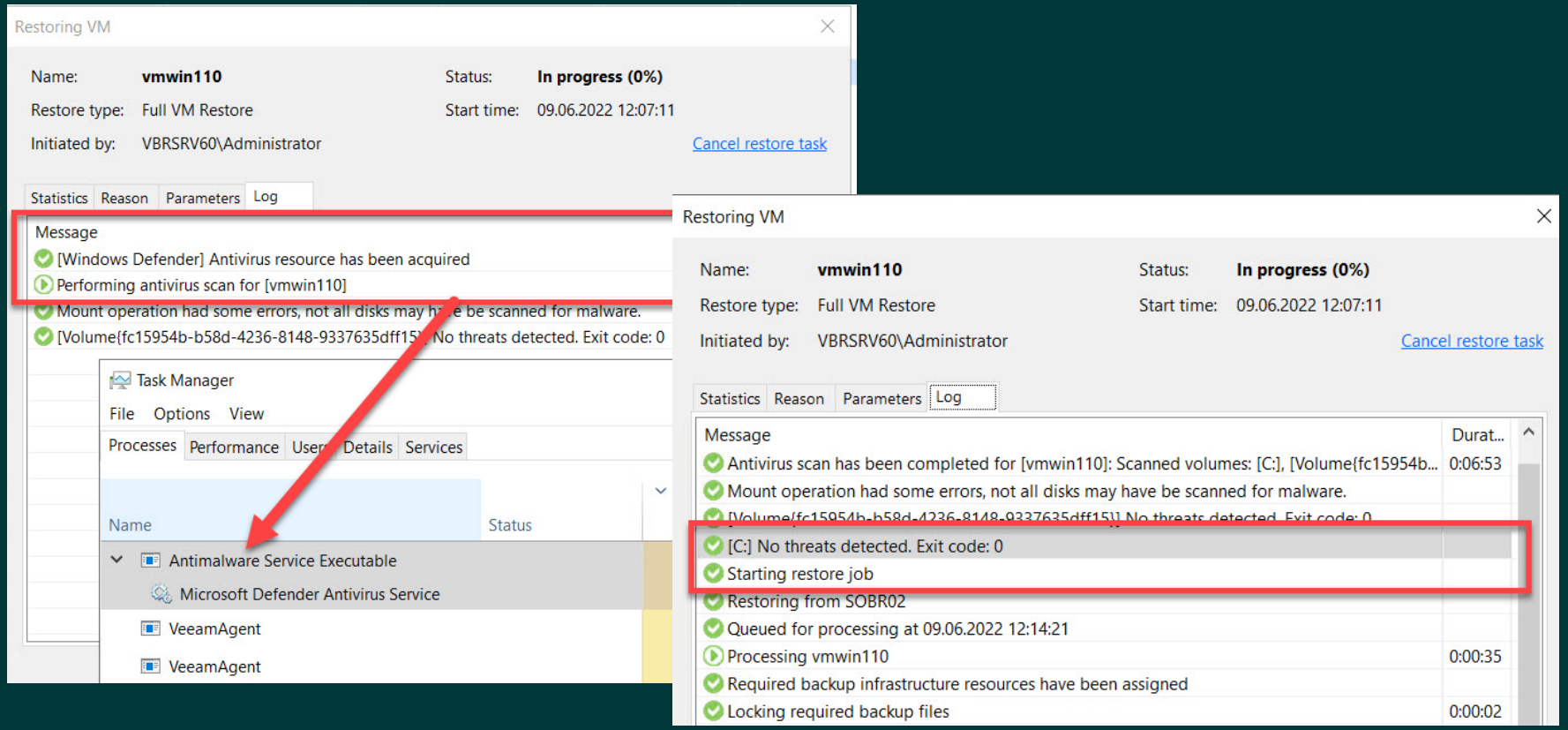
Vermeidet erneuten Kontakt mit Schwachstelle, durch die Zero-Day-Lücken ausgenutzt werden können



Immens wichtig für eine schnelle Wiederherstellung ist die Auswahl einer Backup-Version vor der der heruntergeladenen Datei, die somit kein Risiko darstellt.

Backup in isolierter Umgebung und mit Virenschutz-Prüfung (nach aktuellem Kenntnisstand).

Sichere Wiederherstellung



VEEAM

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 Immutibility 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!

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