



Alternative zum bisherigen Hypervisor?

Multi-Platform Backup & DR & Malware Protection



Marco Horstmann

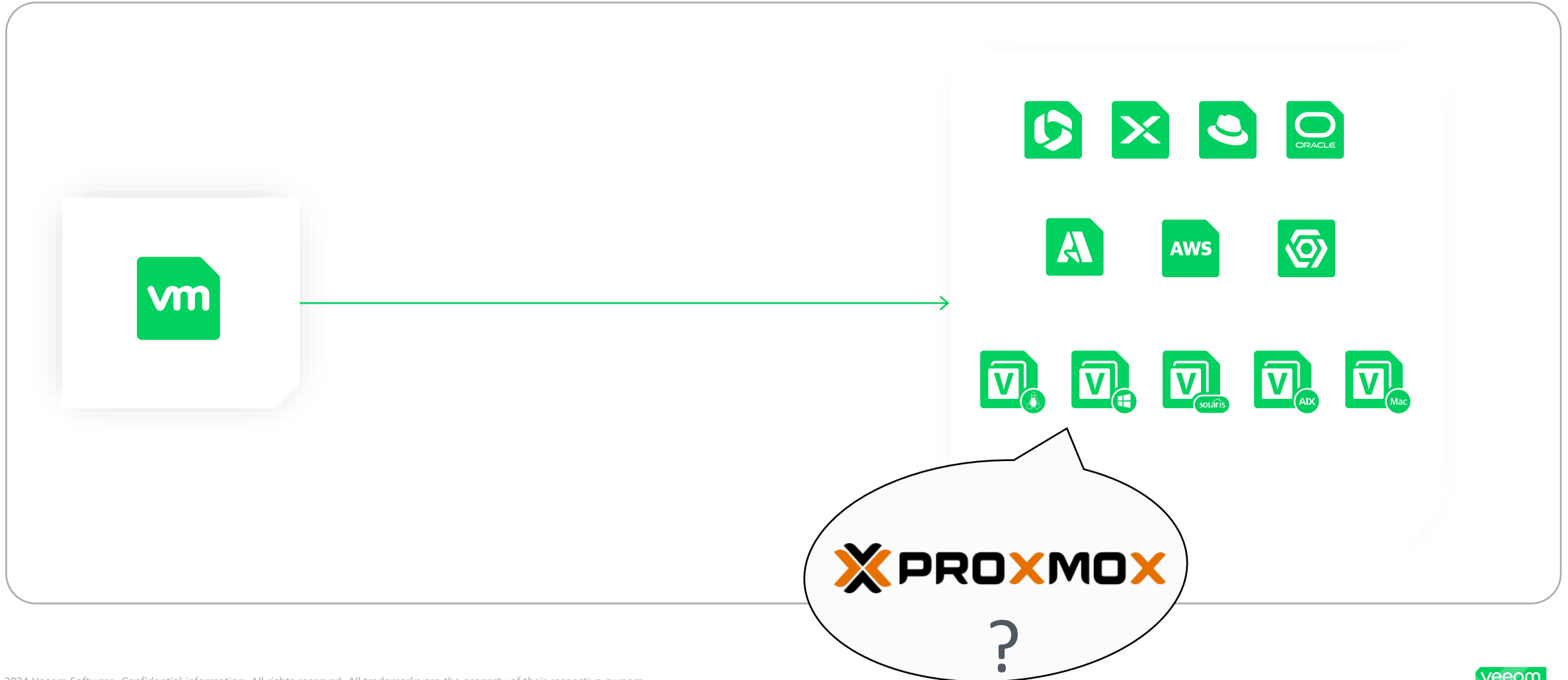
Senior Systems Engineer



Was auch immer Kunden planen, es gibt einen Weg, wie Veeam sie unterstützen kann!

Das Kundenumfeld ändert sich ständig...

...und wir auch



#veeamon

veeamon 24

JUNE 3-5 | FORT LAUDERDALE, FL & ONLINE

Scannen zum
Registrieren



veeamon.com

Fragen der Kunden

Wie können sie ihre Systeme auf eine neue Plattform migrieren?

Benötigen sie eine neue Backup-Lösung?

Können sie ihre bestehenden Backups wiederherstellen?



Veeam Data Platform

Recovery Orchestration

Monitoring & Analytics

Backup & Recovery

Native APIs

Platform
Extensions

 AWS
 Azure
 Google Cloud
 Kubernetes



Cloud



Virtual



Physical



Apps



SaaS

 Microsoft 365
 Salesforce

On-Premises · In the Cloud · XaaS

Kunden benötigen eine Veeam Universal License (VUL)!

Nur VUL bietet Freiheit und Flexibilität

Mit VUL können Kunden Backups erstellen:

Virtuell: VMware, Hyper-V, Nutanix AHV & Red Hat / Oracle Virtualisierung

Cloud: AWS, Microsoft Azure und Google Cloud

Physische Server und Workstations: Windows, Linux, Mac, IBM AIX und Oracle Solaris

Unternehmensanwendungen: Oracle, SAP, SQL, ...

NAS & Objektspeicher



Schützt alle Workloads
Übertragbar!
Flexibel!
Einfacher denn je!

Multi-Platform Backup & DR – Image-Level

Mit Veeam können Workloads von On-Premises zu Cloud, aber auch von Cloud zu Cloud, Cloud zu On-Premises, virtuell zu virtuell wiederhergestellt werden,....



Multi-Platform Backup & DR – File/Application-Level

Auch Datei- und Anwendungs-Backups können flexibel wiederhergestellt werden

Datei-/NAS-Backups auf verschiedene Ziele wiederherstellen

Objektspeicher zwischen verschiedenen Anbietern und Protokollen (Beispiel: AWS <> Azure)

Datenbanken auf verschiedenen Servern/Umgebungen

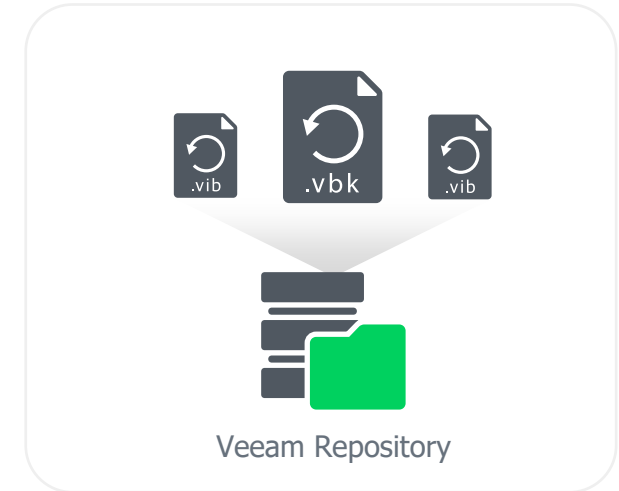
E-Mails von Exchange Online zu Exchange on-premises

Backup Mobility



Kunden kontrollieren und besitzen ihre Backup-Daten!

Veeam Backup & Replication verwendet ein portables Dateiformat, das es Kunden ermöglicht, Backups dort zu speichern, wo sie es wünschen, und mehrere Wiederherstellungsmöglichkeiten anzubieten



Flexibel

Das portable Sicherungsformat ermöglicht es den Kunden, ihre Sicherungsdaten sicher und zuverlässig zu verschieben.

Dies ermöglicht Kopien außerhalb des Standorts oder Datenmigrationen und trägt zur Einhaltung der 3-2-1-1-0-Regel bei.

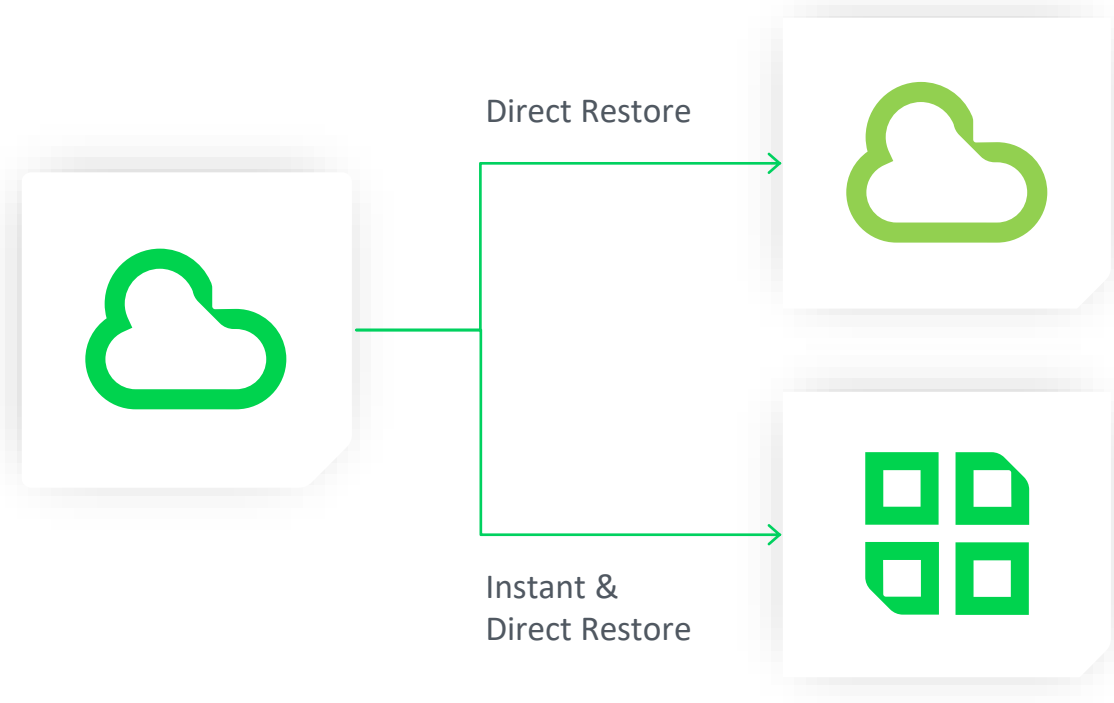
Sicher

Kunden können ihre Sicherungsdaten durch Verschlüsselung und Unveränderlichkeit schützen

Kein Vendor Lock-In

Backup-Daten sind immer zugänglich, unabhängig davon, ob Kunden auf andere Plattformen oder Clouds migrieren

Kunden-Szenario



Veeam's Solution

Systeme aus Cloud "A" in Cloud "B" können direkt wiederhergestellt werden

Systeme aus der Cloud "A" in eine neue Virtualisierungslösung "C":

- über Direct Restore
- über Instant Recovery

Die Lösung von Veeam

Können wir Daten auf neue Plattformen migrieren?

- Ja, abhängig von der Quelle und dem Ziel

Benötigen die Kunden neue Sicherungslösungen?

- Nein, nicht, wenn wir die neue Plattform unterstützen.
- Behalten Sie Veeam Agents im Hinterkopf!

Können bestehende Backups weiter verwendet/wiederhergestellt werden?

- Ja, wir benötigen die Quellinfrastruktur nicht zur Wiederherstellung



Was können wir den Kunden
sonst noch bieten?

Was sonst noch?



Freie Wahl bei Anbietern und Technologien



Disaster Recovery auf verschiedenen Plattformen und Clouds



Migration von Arbeitslasten, aber auch Ausstiegsstrategie



“Data Reuse”



Flexible Lizenzierung



Instant Recovery, nicht nur für Image-Backups



Schnellere Anpassung an Veränderungen

Kein Vendor Lock-In

Veeam ist eine Softwarelösung

Wechsel des Server- und Storage-Anbieters

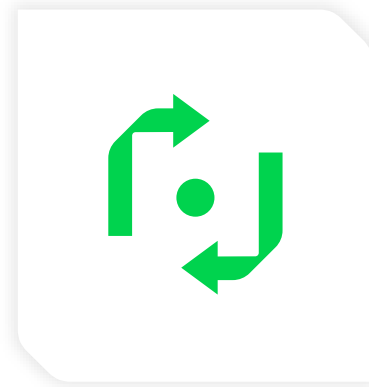
Wechsel der Speichertechnologie:

- Block -> Object Storage
- On-Premises -> Cloud
- Deduplication Appliance

Wechsel des Cloud- und Virtualisierungsanbieters



Kein „Veeam“ Lock-In

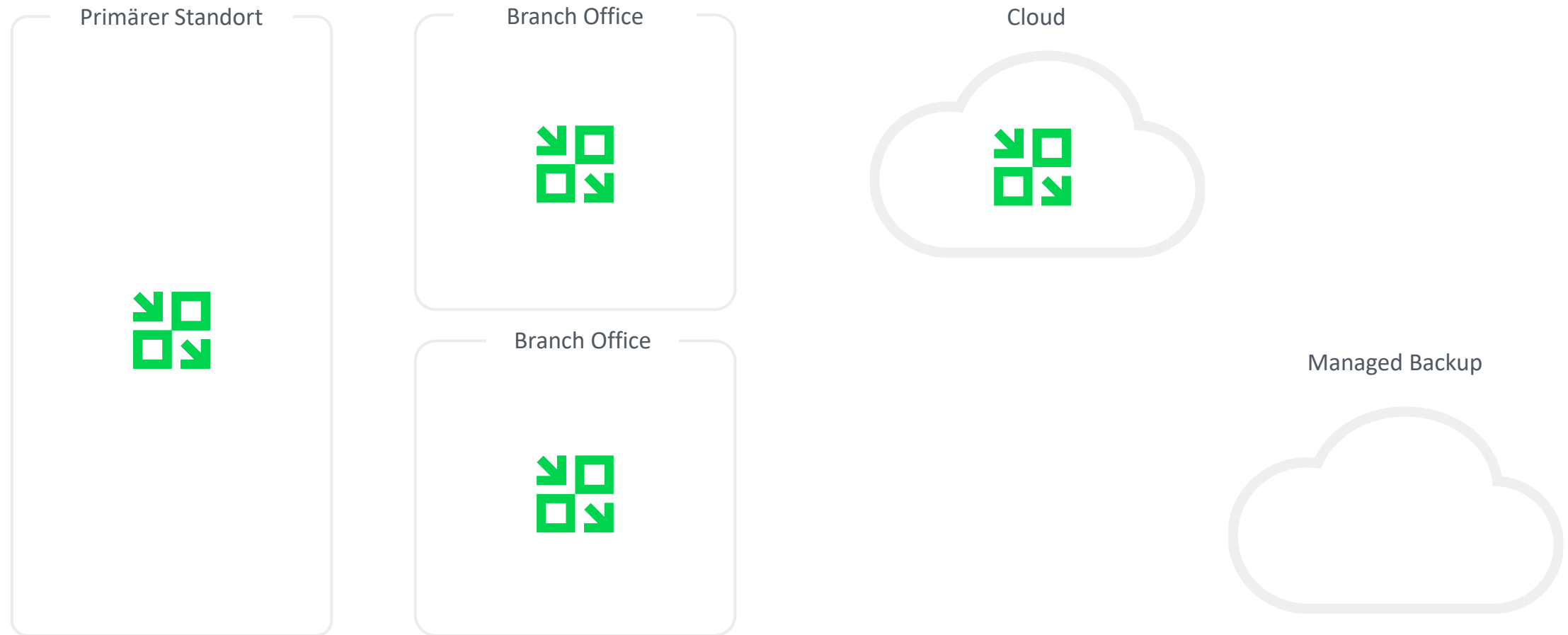


Der Zugriff auf Backups ist auch ohne aktive Veeam-Installation möglich

- Extract Utility
- Community Edition

Freie Wahl des Sicherungsortes

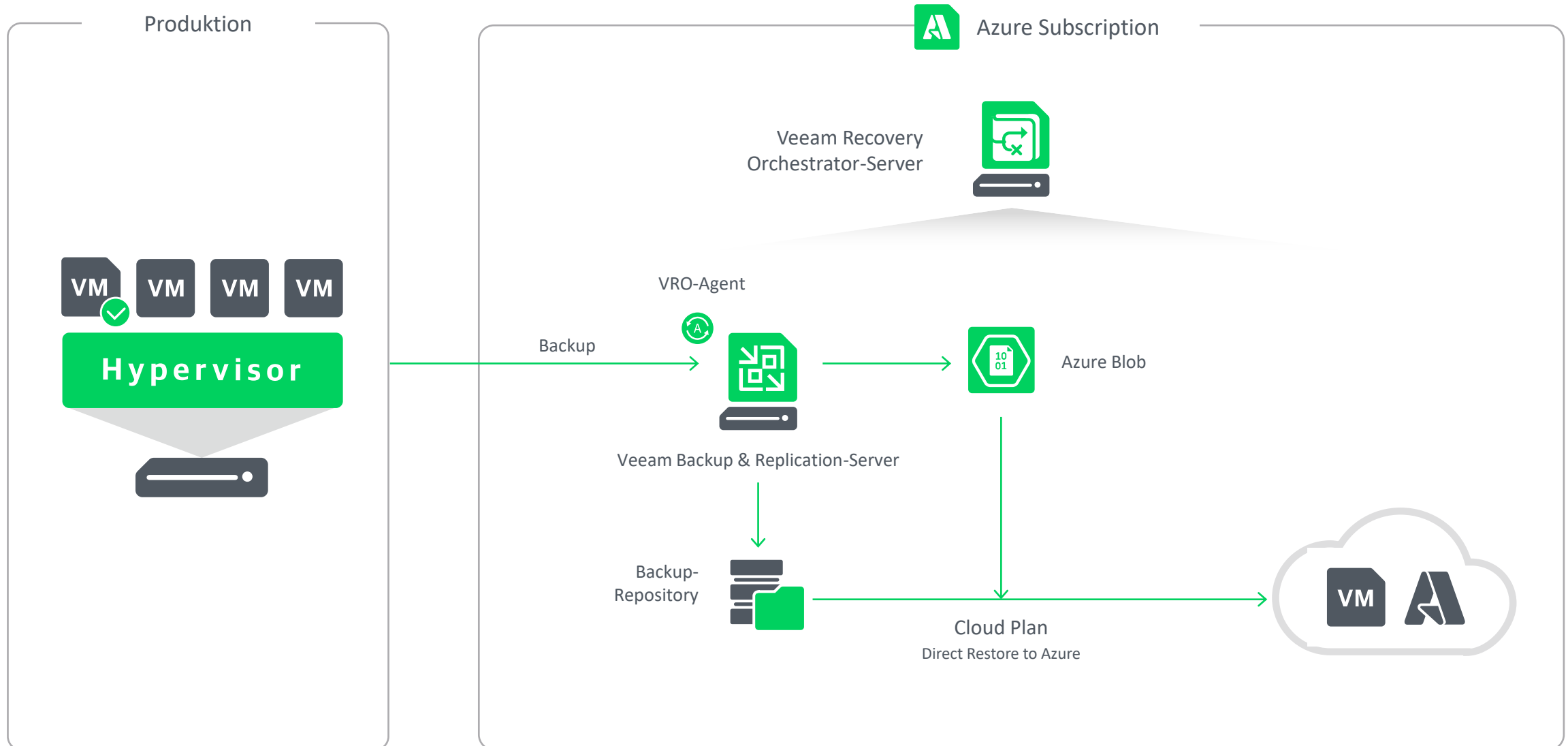
On-Premises, Hybrid, Cloud, Managed Backup....





Vergessen Sie nicht Veeam
ONE, Recovery
Orchestrator oder
Veeam Data Cloud!

Orchestrierte Wiederherstellung in Azure



Um es zusammenzufassen...

... mit Veeam können Kunden:

- Schutz verschiedener Arbeitslasten und Plattformen
- flexibel wiederherstellen können, wie sie wollen
- keine Einschränkungen von Veeam beim Aufbau ihrer Backup-Infrastruktur haben
- über ihre Sicherungsdaten verfügen
- Unterstützung neben der Sicherung und Wiederherstellung erhalten



Warum Malware Detection beim Backup?

Section 1

Besser spät als nie!

Warum Malware Detection beim Backup?

Was bringt es an dieser Stelle und was nicht

- Erkennen von Malware beim Backup ist etwas spät.
Besser spät als zu spät!
- Veeam Malware Detection ersetzt keine andere Lösung.
Ist als zusätzliches Hilfsmittel zu betrachten.
- Detection Algorithmen benötigen nur Ressourcen in der Backup Infrastruktur.

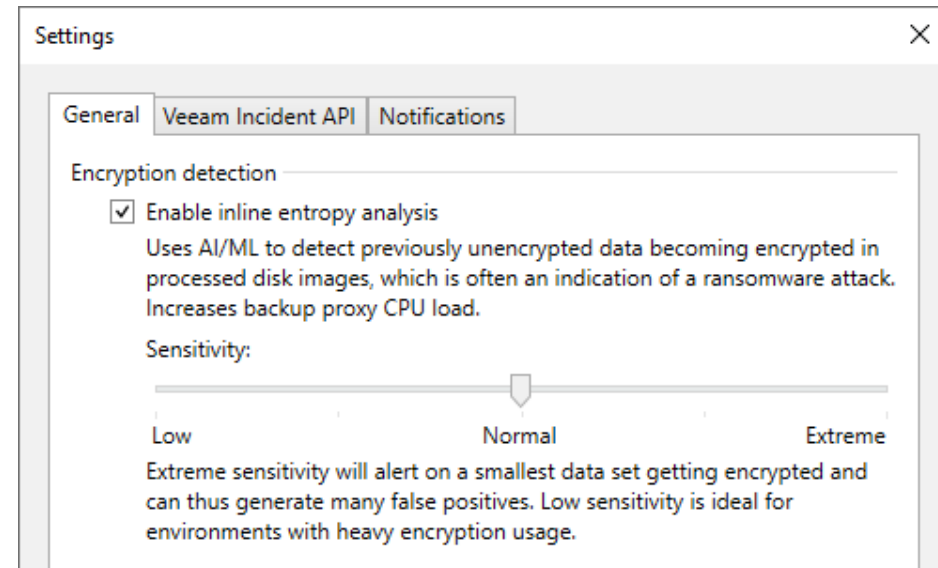
Detection Methoden

Section 2
Wie wird Malware
gefunden

Malware Detection Methoden

Inline Detection – Encryption Detection

- Blocklevel-Analyse während des Backups (am Proxy)
- Entropie-Analyse
 - AI/ML
 - Detektiert verschlüsselte Daten
 - Sensitivität konfigurierbar
 - Full-read nach Aktivierung
 - Höhere CPU-Last

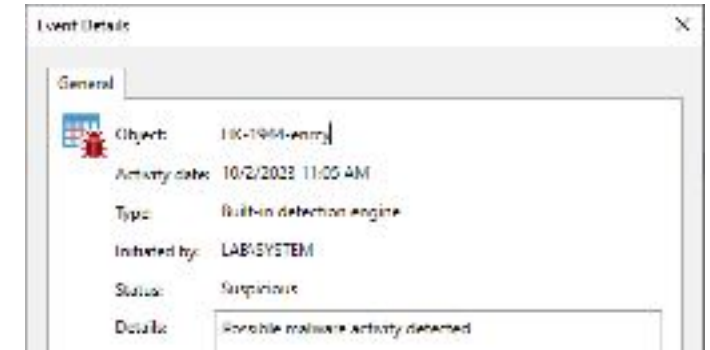


Malware Detection Methoden

Inline Detection – How **Encryption Detection** works

- Während des Backups

- Sammeln Metadaten und Statistiken über Backupdaten
- *Magic*-Wert Berechnung



- Nach dem Backup

- Speichern Metadaten und Statistiken in VBRcatalog (nicht verwechseln mit Guest Indexing; <1MB/1M Files)
- Vergleich mit vorherigen Daten



Malware Detection Methoden

Inline Detection – How **Encryption Detection** works

Cross-Correlation zwischen aktuellen und historischen Werten

(Beispiel)Daten für die Berechnung

- Incremental Backup Größe
- Encryption (Absolute Größe & Prozent)
- Compression
- Magic decrement (Daten gelöscht)
- Magic encryption (Neu verschlüsselte Daten)
- Ransom notes found

Malware Detection Methoden

Guest Indexing

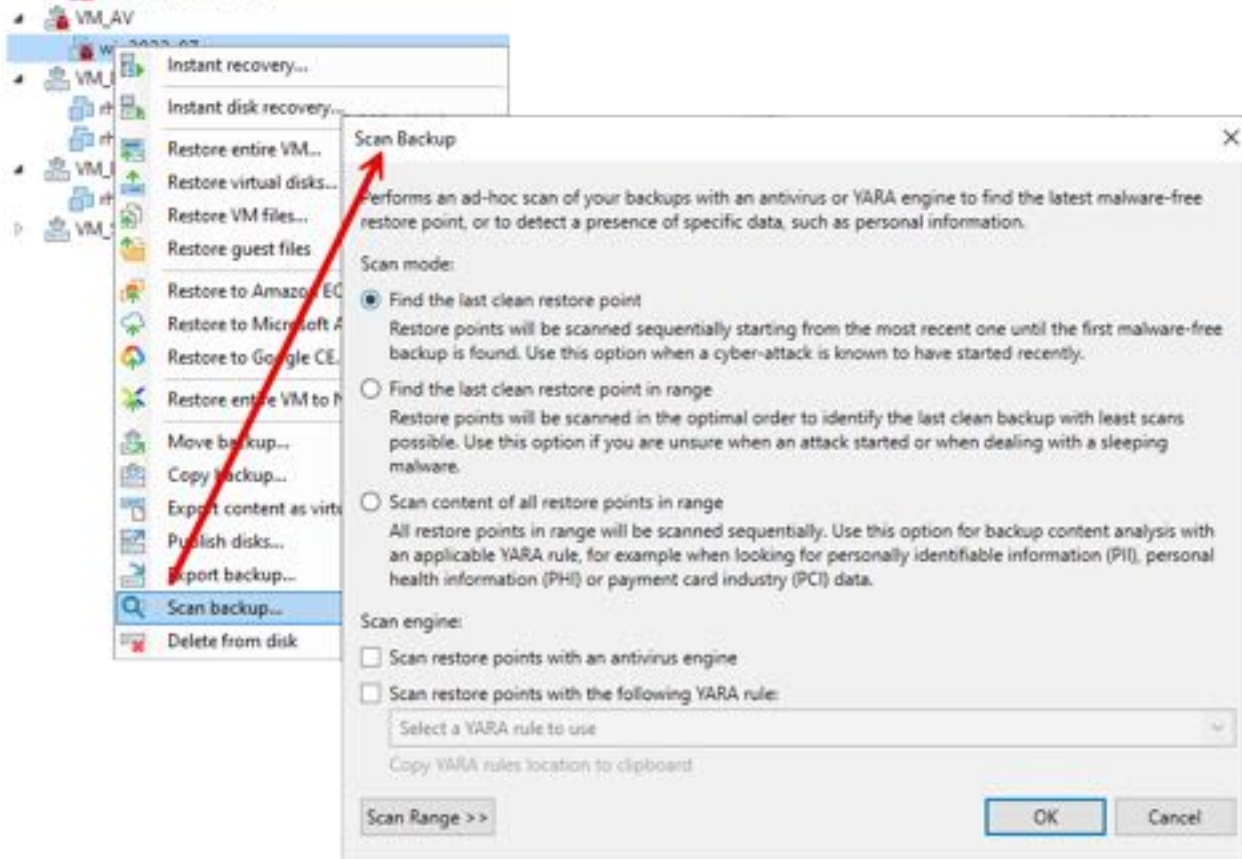
- Erkennen von verschlüsselten Files anhand File-Extension
 - >4k pre-defined (SuspiciousFiles.xml)
 - Algorithmen für unbekannte Extensions
 - Manuelles Überschreiben möglich
- Erkennen von Malware Binaries
- Vergleich mit Index älterer Backups (default 24h)



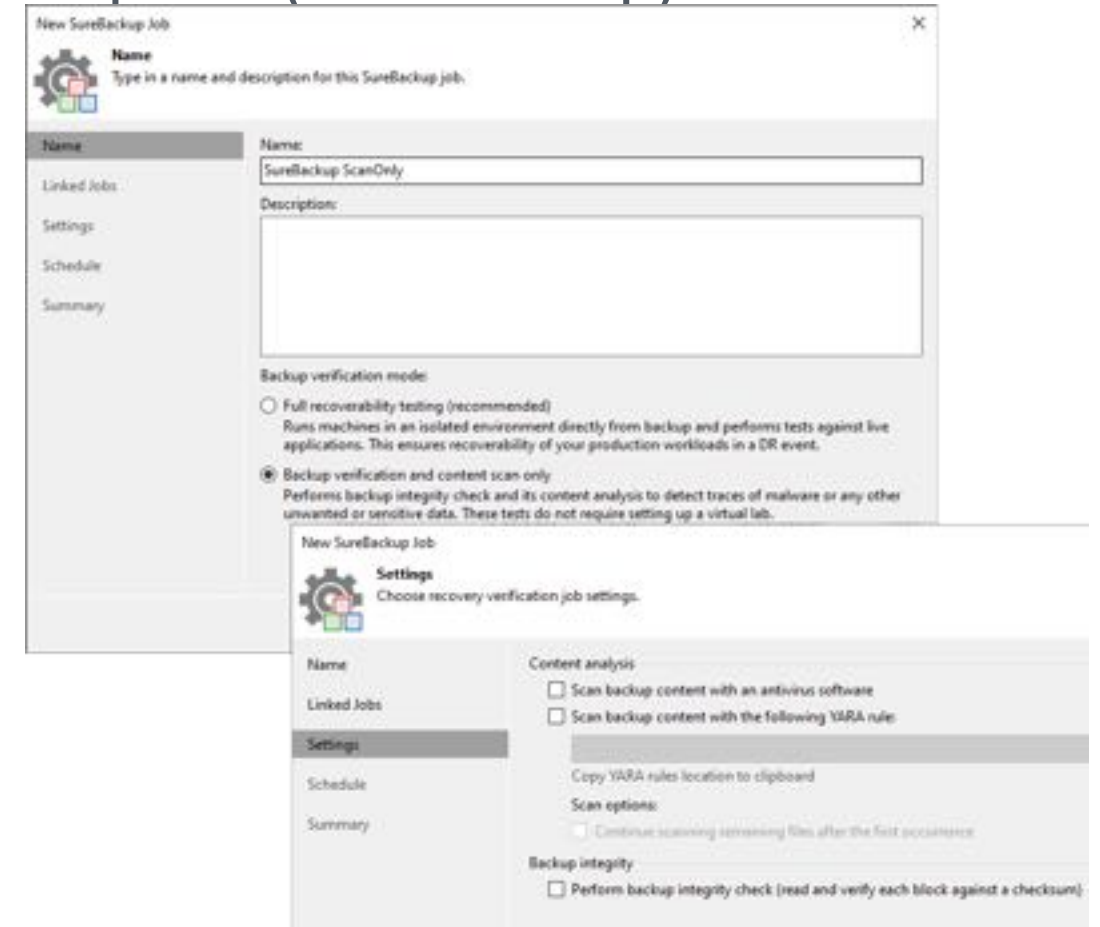
Malware Detection Methoden

On Demand Scan

Manuell



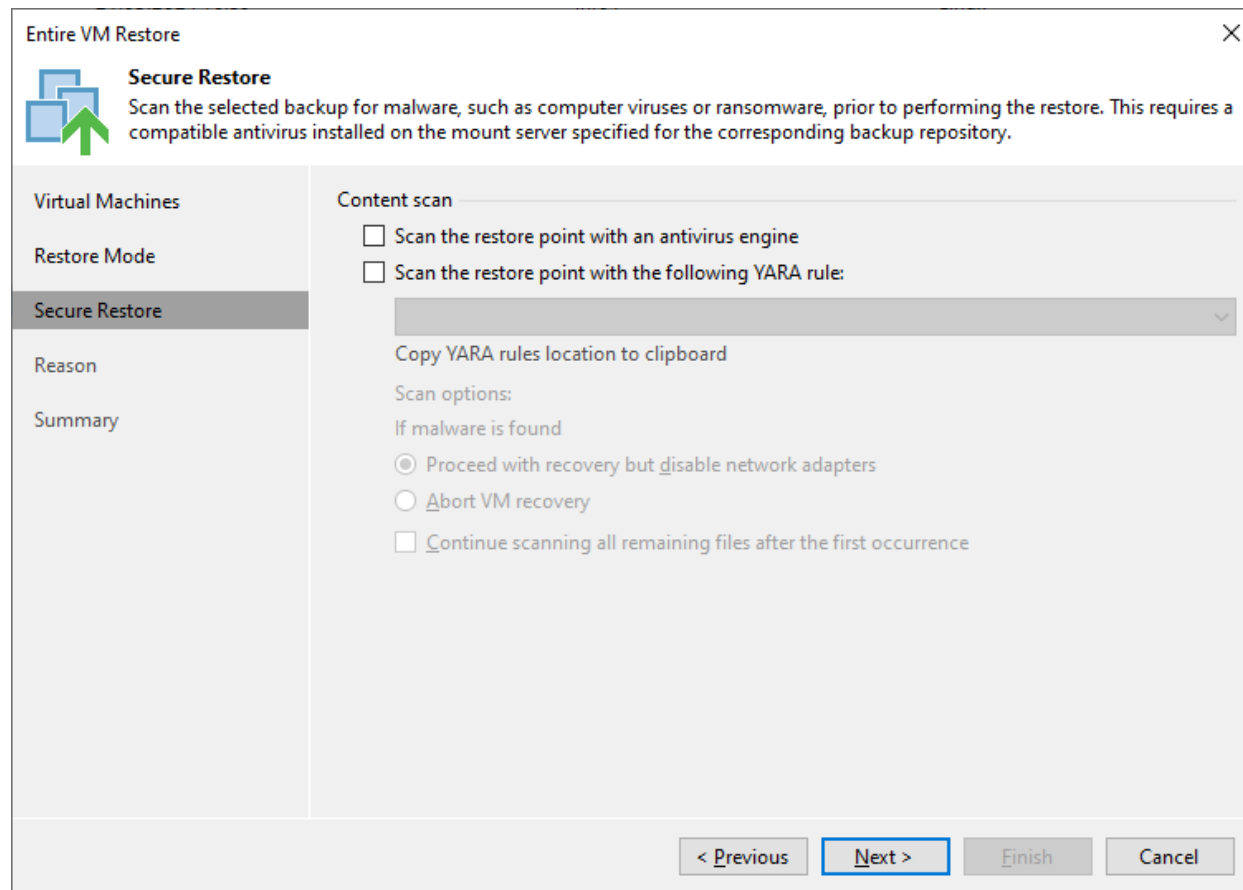
Geplant (SureBackup)



Malware Detection Methoden

On Demand Scan

und natürlich Secure Restore



Entire VM Restore

Secure Restore
Scan the selected backup for malware, such as computer viruses or ransomware, prior to performing the restore. This requires a compatible antivirus installed on the mount server specified for the corresponding backup repository.

Virtual Machines

Restore Mode

Secure Restore

Reason

Summary

Content scan

- Scan the restore point with an antivirus engine
- Scan the restore point with the following YARA rule:
[Dropdown menu]

Copy YARA rules location to clipboard

Scan options:

If malware is found

- Proceed with recovery but disable network adapters
- Abort VM recovery
- Continue scanning all remaining files after the first occurrence

< Previous **Next >** Finish Cancel

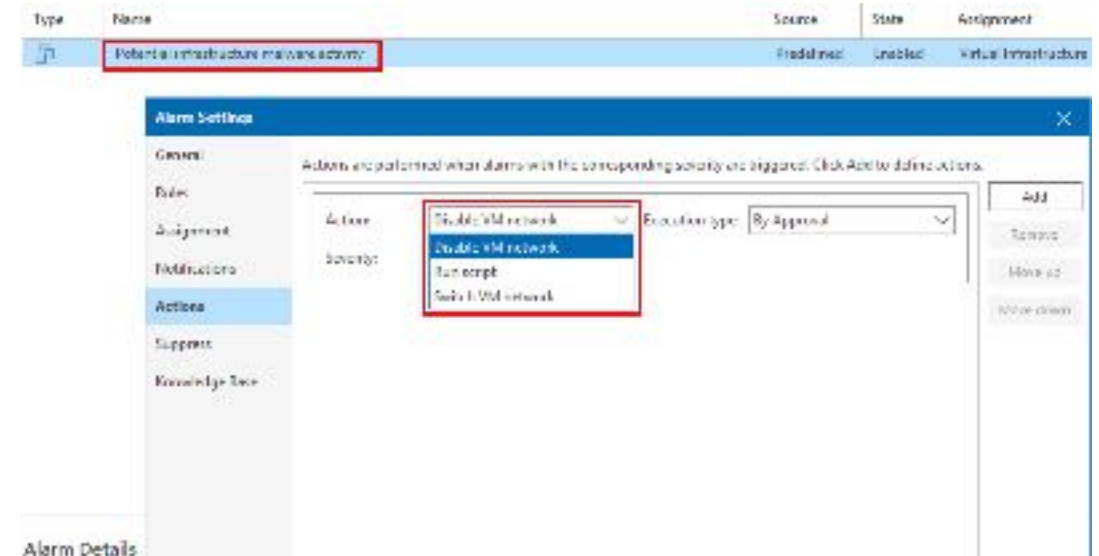
Malware Detetion in Veeam ONE

Section 3
Wie kann Veeam
ONE helfen

Malware Detection in Veeam ONE

Neue Alarme

- vSphere Alarm
 - *Potential infrastructure malware activity*
 - Automatische Aktionen
 - *Disable VM Network*
 - *Switch VM Network*
- Backup & Replication Alarme
 - *Potential malware in backups*
 - *Veeam malware detection activity state*
 - Überwacht, ob Malware Detection deaktiviert wurde
 - *Veeam malware detection exclusions change tracking*
 - Überwacht Malware Detection Ausnahmen-Konfiguration
 - *Veeam malware detection change tracking*
 - Überwacht Malware Detection Einstellungen



Malware Detection in Veeam ONE



Neuer Report

Malware Detection Report

Malware Detection

Description

Top 5 hosts with most malware events detected in the last 24 hours. This report shows the top 5 hosts with the most malware events detected in the last 24 hours. The report is generated by the Veeam ONE console.

Report Parameters

Scope: Backup Infrastructure
 Malware Status: All
 Hosts to Show: 5

Summary

Malware analysis workload

Total events: 10
 Detected: 1
 Suspicious: 1
 Not analyzed: 8

Malware analysis malware points

Total malware points: 100
 Detected: 5
 Suspicious: 10
 Not analyzed: 85

Top 5 hosts with most malware events

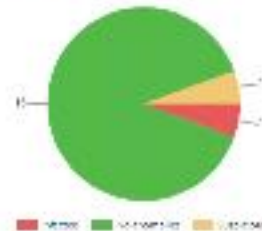
Backup Owner	Supplines	Infected
Host1	1	1

Details

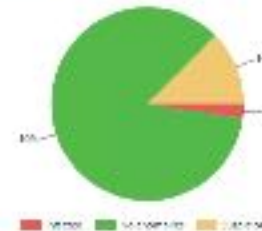
Backup server: Host1

Malware Name	Location	Transfer Dates	Learning Percentage	Status	Event Parameters	Description	Event Type
Worm:MSL	C:\Program Files\Microsoft Office\Office16\	2024-10-24 08:00:00	100%	Detected	File: C:\Program Files\Microsoft Office\Office16\MSL.exe	Malware detected in the backup image. The file is a known malware.	Malware
Worm:MSL	C:\Program Files\Microsoft Office\Office16\	2024-10-24 08:00:00	100%	Detected	File: C:\Program Files\Microsoft Office\Office16\MSL.exe	Malware detected in the backup image. The file is a known malware.	Malware
Worm:MSL	C:\Program Files\Microsoft Office\Office16\	2024-10-24 08:00:00	100%	Detected	File: C:\Program Files\Microsoft Office\Office16\MSL.exe	Malware detected in the backup image. The file is a known malware.	Malware
Worm:MSL	C:\Program Files\Microsoft Office\Office16\	2024-10-24 08:00:00	100%	Detected	File: C:\Program Files\Microsoft Office\Office16\MSL.exe	Malware detected in the backup image. The file is a known malware.	Malware

Malware analysis workload



Malware analysis malware points



Top 5 Backup servers with workload events



The Veeam logo is displayed in white lowercase letters within a white-outlined, rounded rectangular frame. The background features a green gradient with abstract, overlapping geometric shapes in various shades of green.

Follow us!



Join the community hub:

