Alternative zum bisherigen Hypervisor?

Multi-Platform Backup & DR & Malware Protection

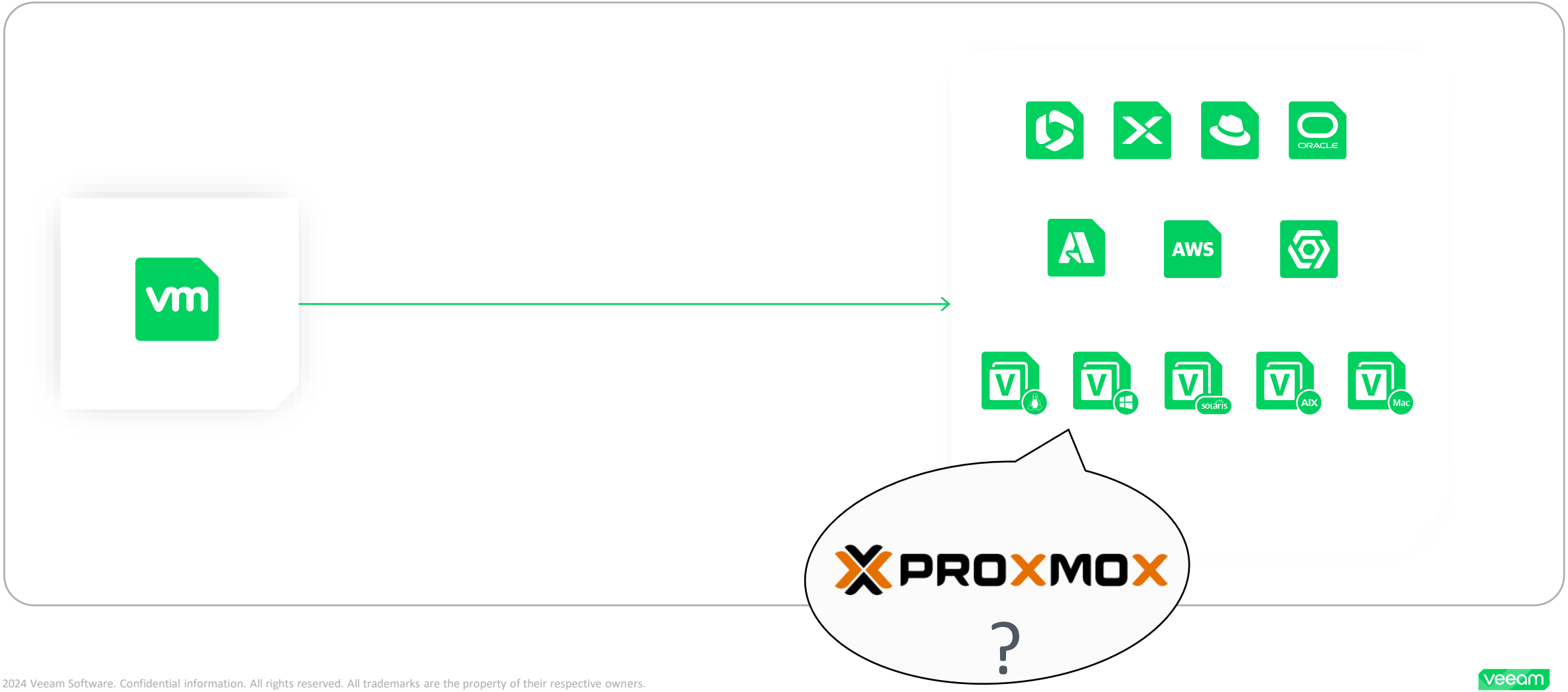
Marco Horstmann

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

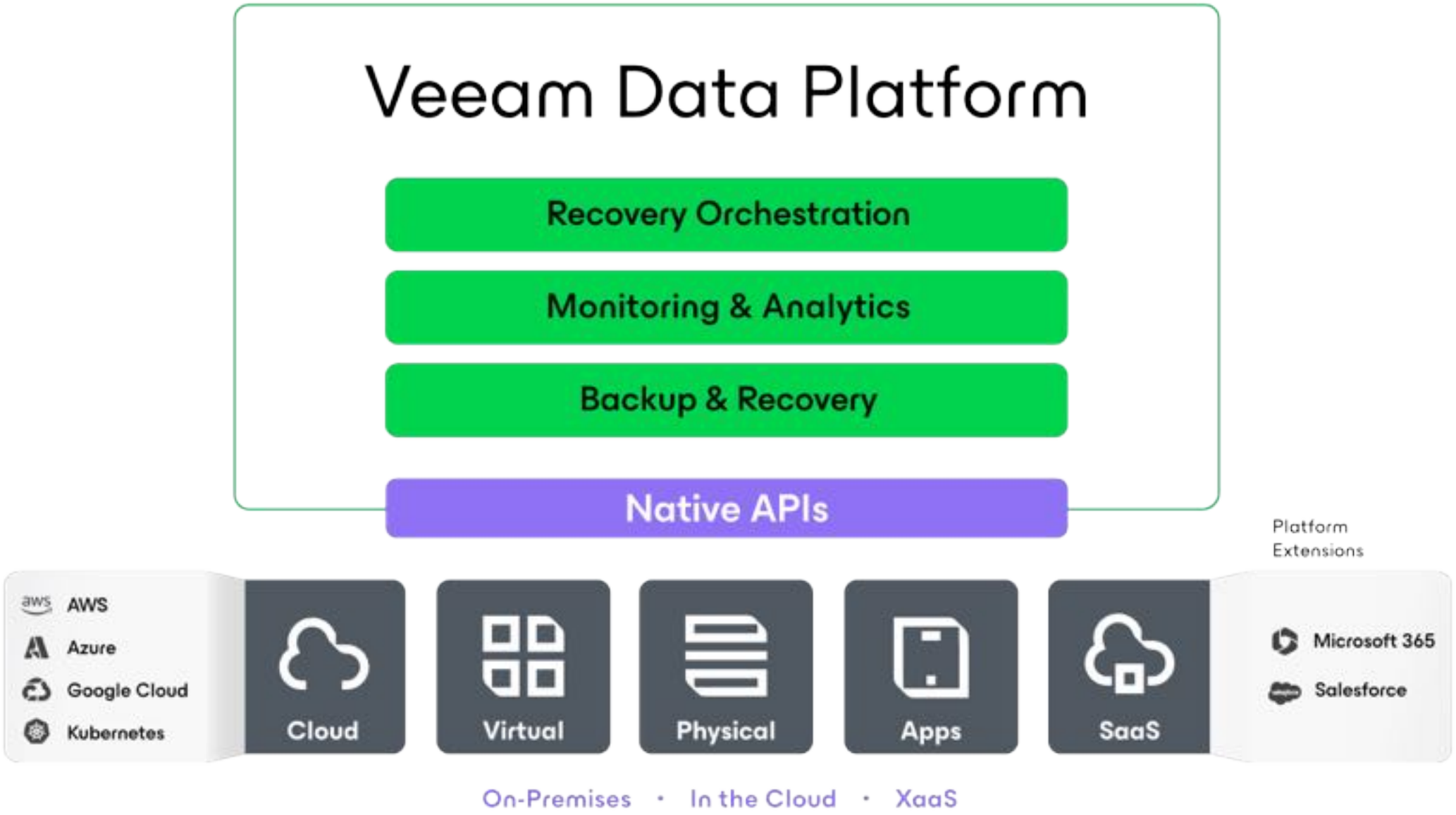
veeamon.com

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?



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)

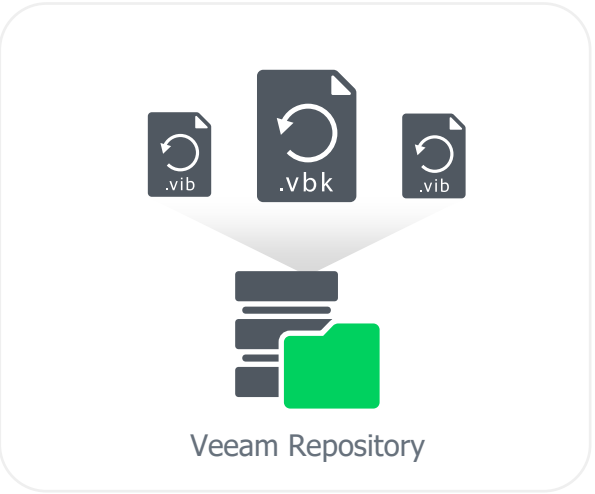
Datenbanken auf verschiedenen Servern/Umgebungen

E-Mails von Exchange Online zu Exchange on-premises

Backup Mobility

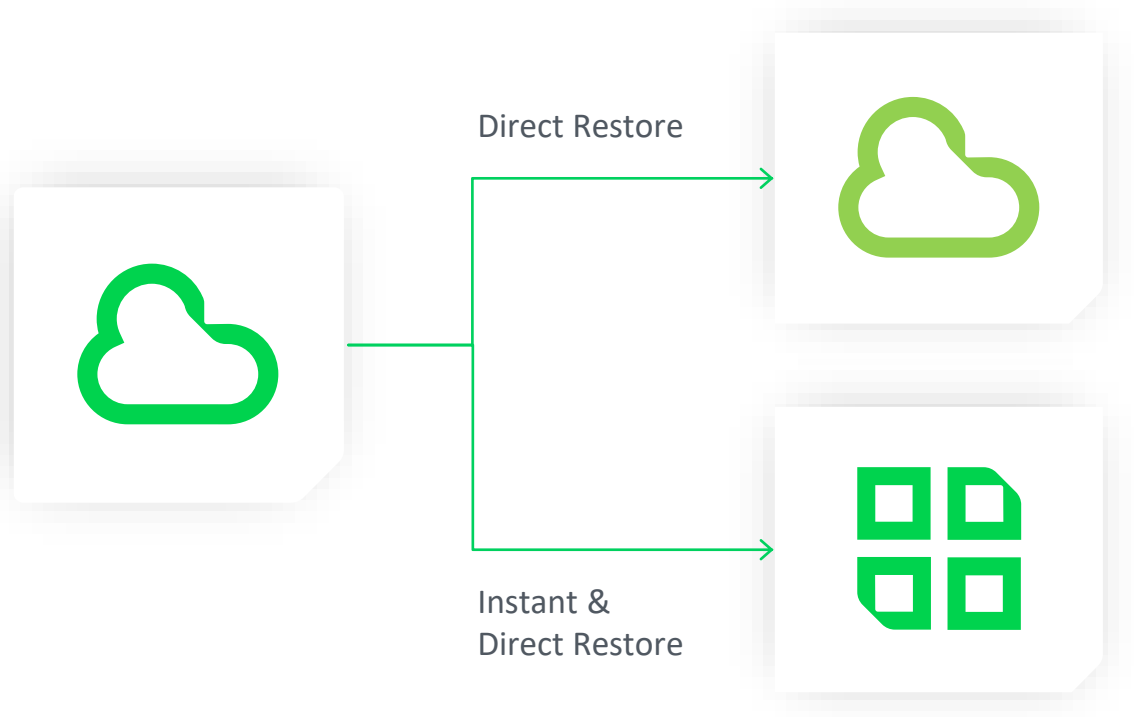
Kunden kontrollieren und besitzen ihre Backup-Daten!

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



Flexibel	Sicher	Kein Vendor Lock-In
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.	Kunden können ihre Sicherungsdaten durch Verschlüsselung und Unveränderlichkeit schützen	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

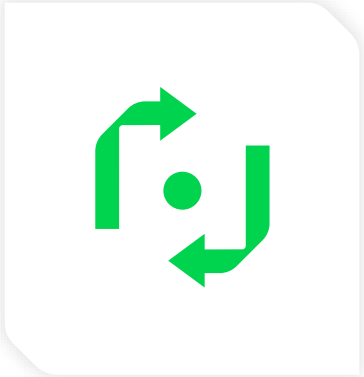
Wechsel des Server- und Storage-Anbieters

Wechsel der Speichertechnologie:

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

Wechsel des Cloud- und Virtualisierungsanbieters

Kein „Veeam“ Lock-In

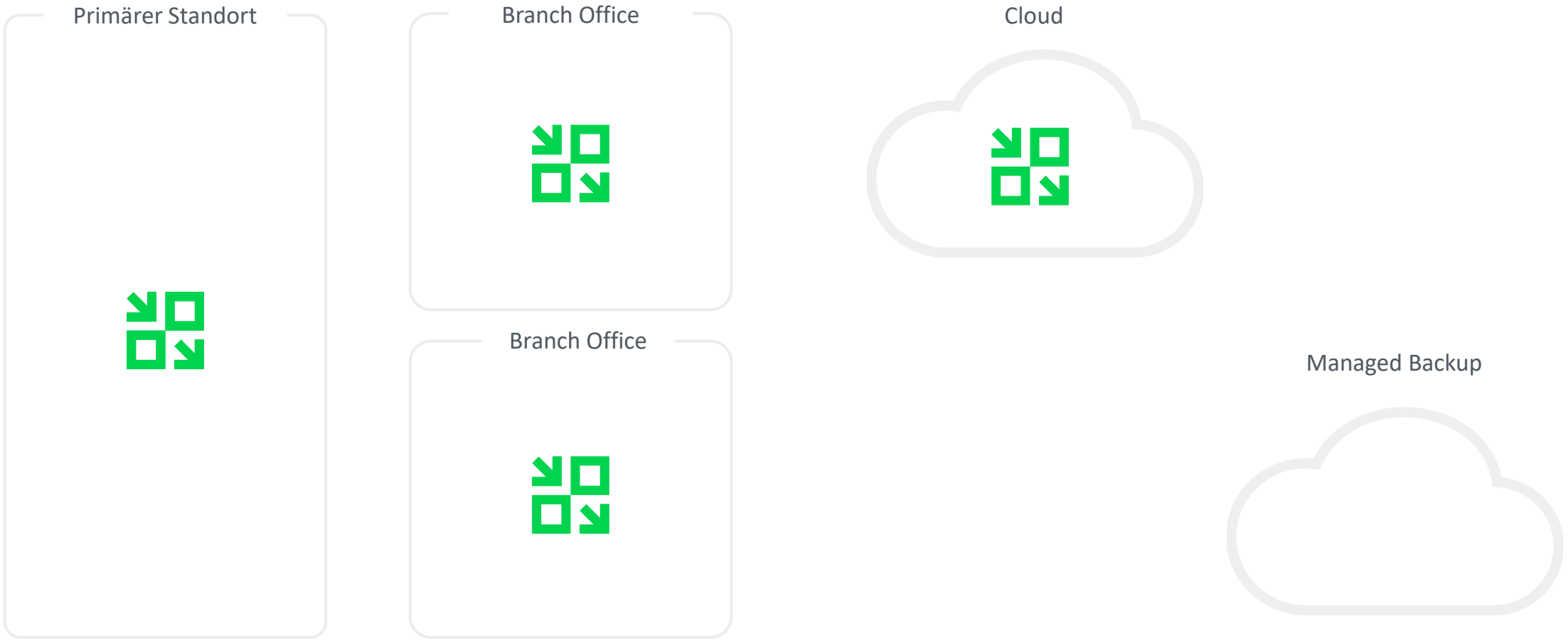


Der Zugriff auf Backups ist auch ohne aktive Veeam-Installation möglich

- Extract Utility
- Community Edition

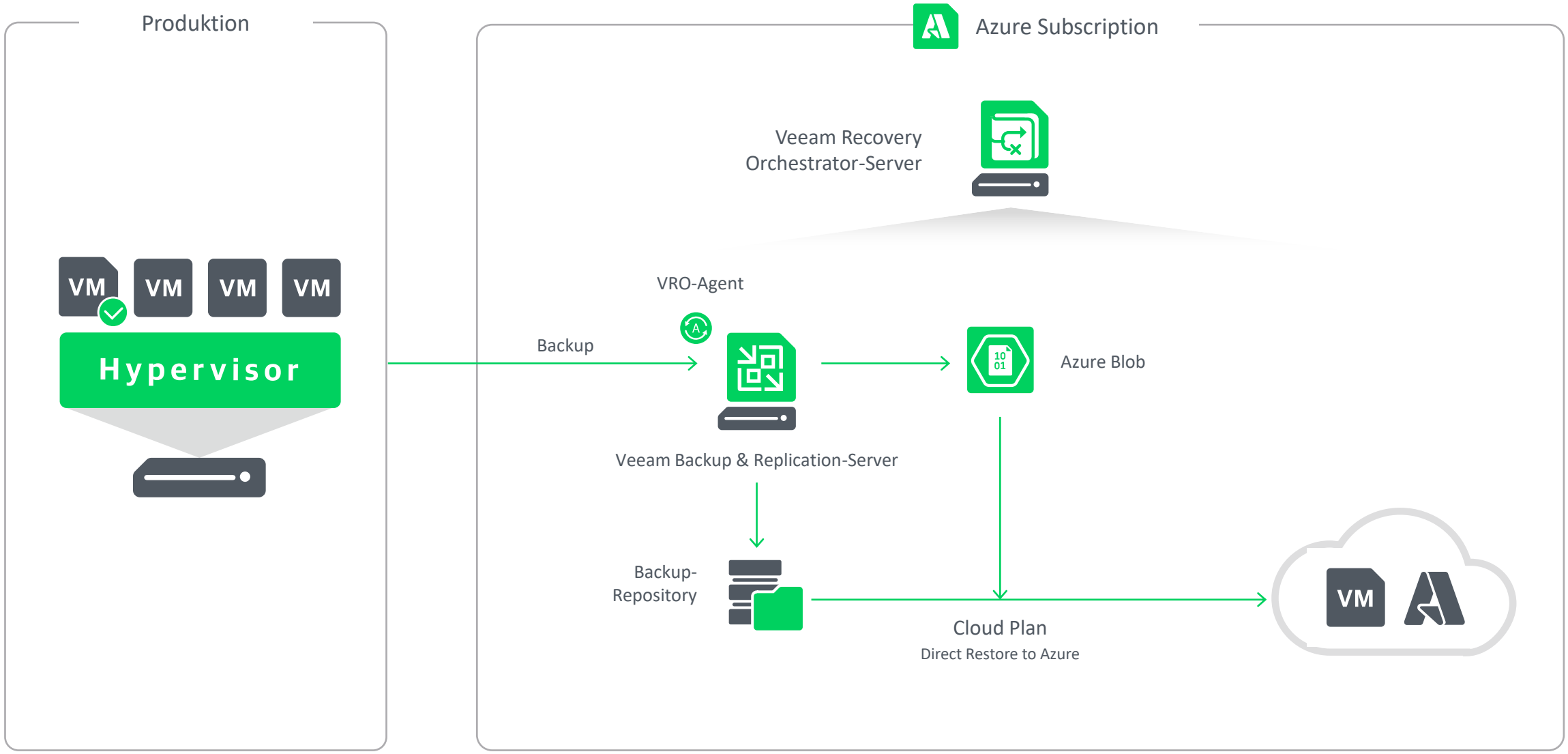
Freie Wahl des Sicherungsortes

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

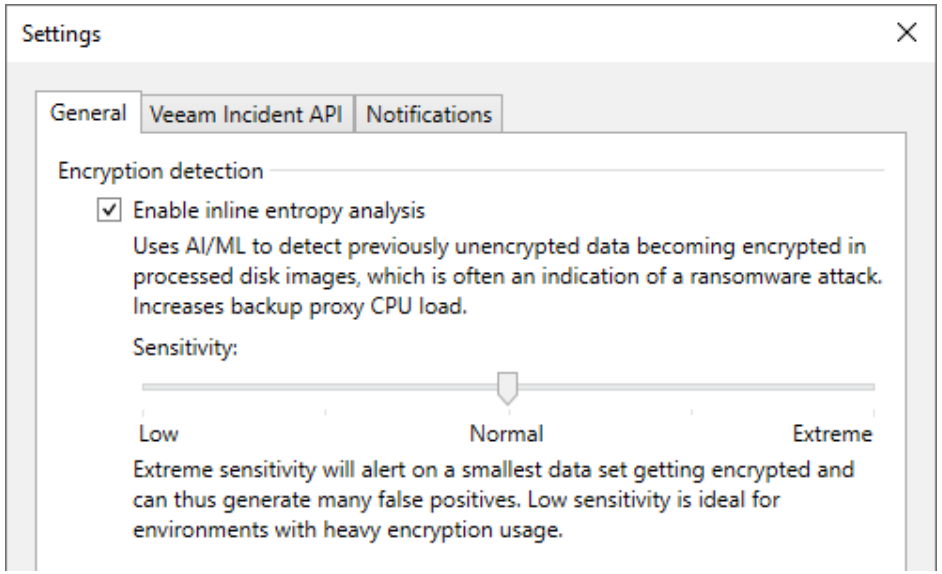
Section 2

Wie wird Malware gefunden

Malware Detection Methoden

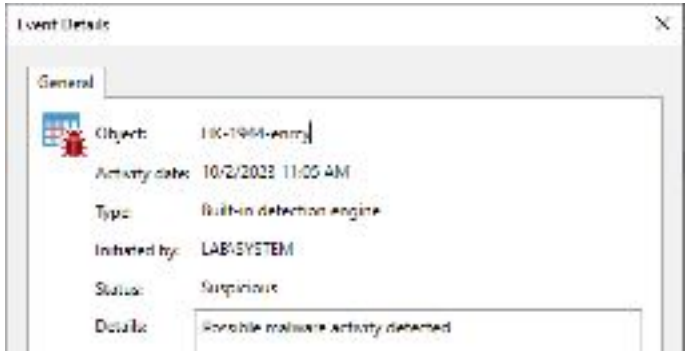
Inline Detection – Encryption Detection

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



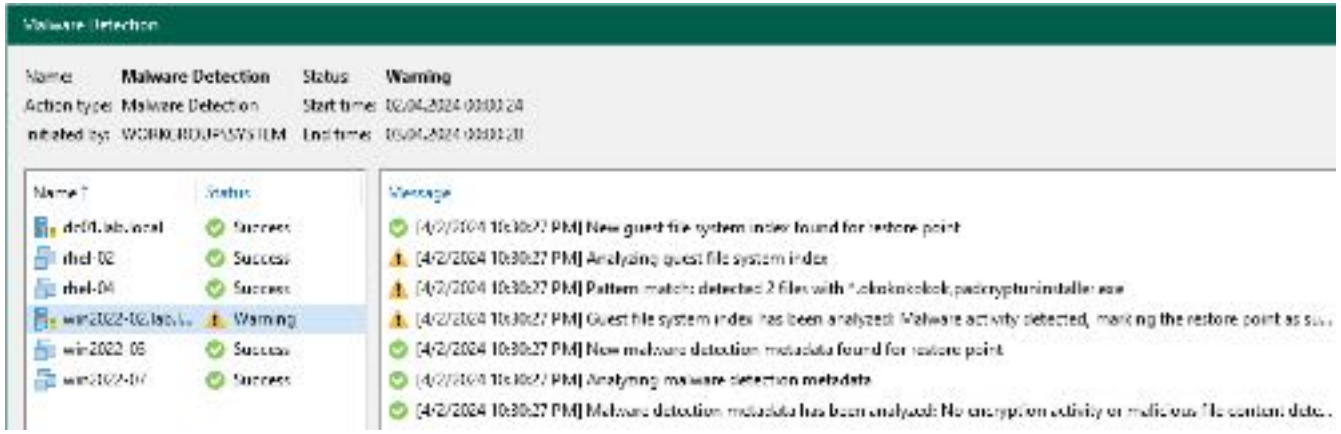
Malware Detection Methoden

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

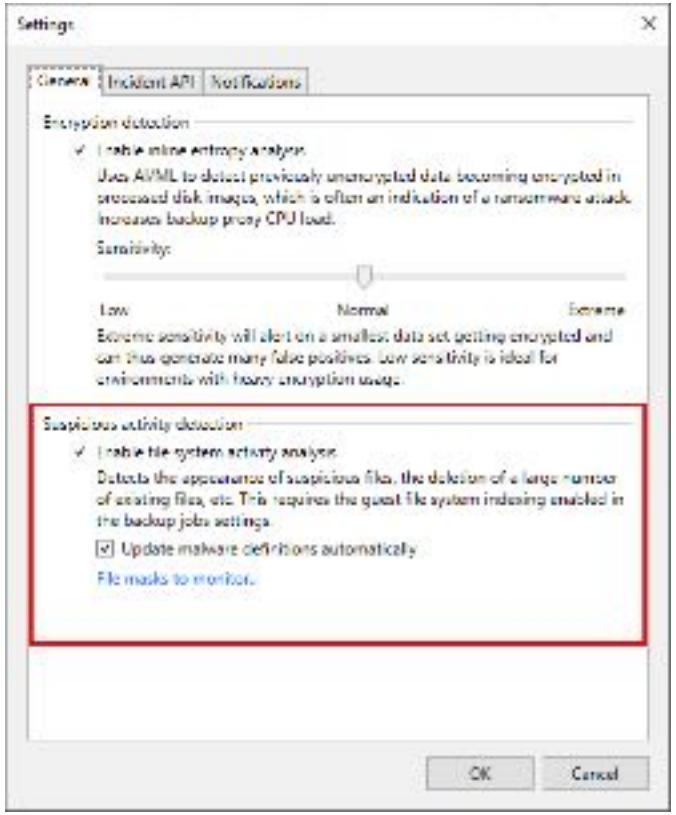
(Beispiel)Daten für die Berechnung

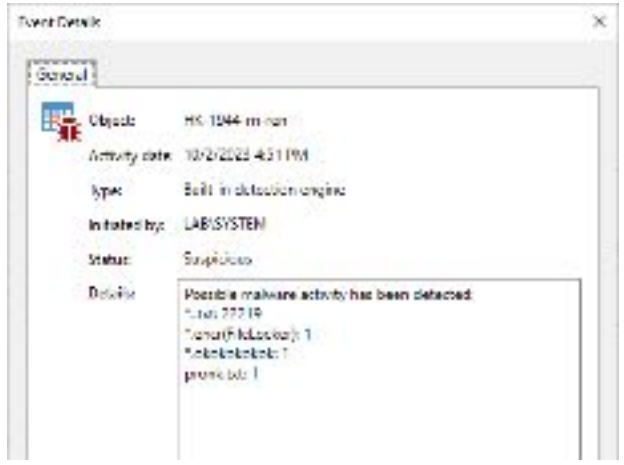
- Incremental Backup Größe
- Encryption (Absolute Größe & Prozent)
- Compression
- Magic decrement (Daten gelöscht)
- Magic encryption (Neu verschlüsselte Daten)
- Ransom notes found

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)

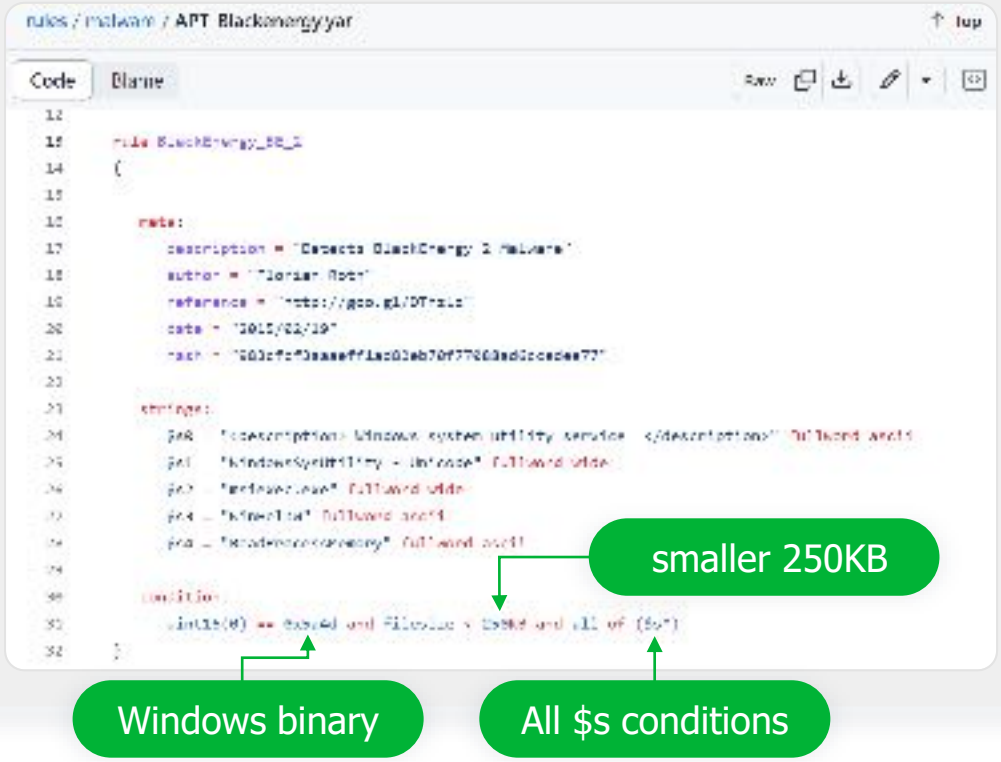




Malware Detection Methoden

On Demand Scan

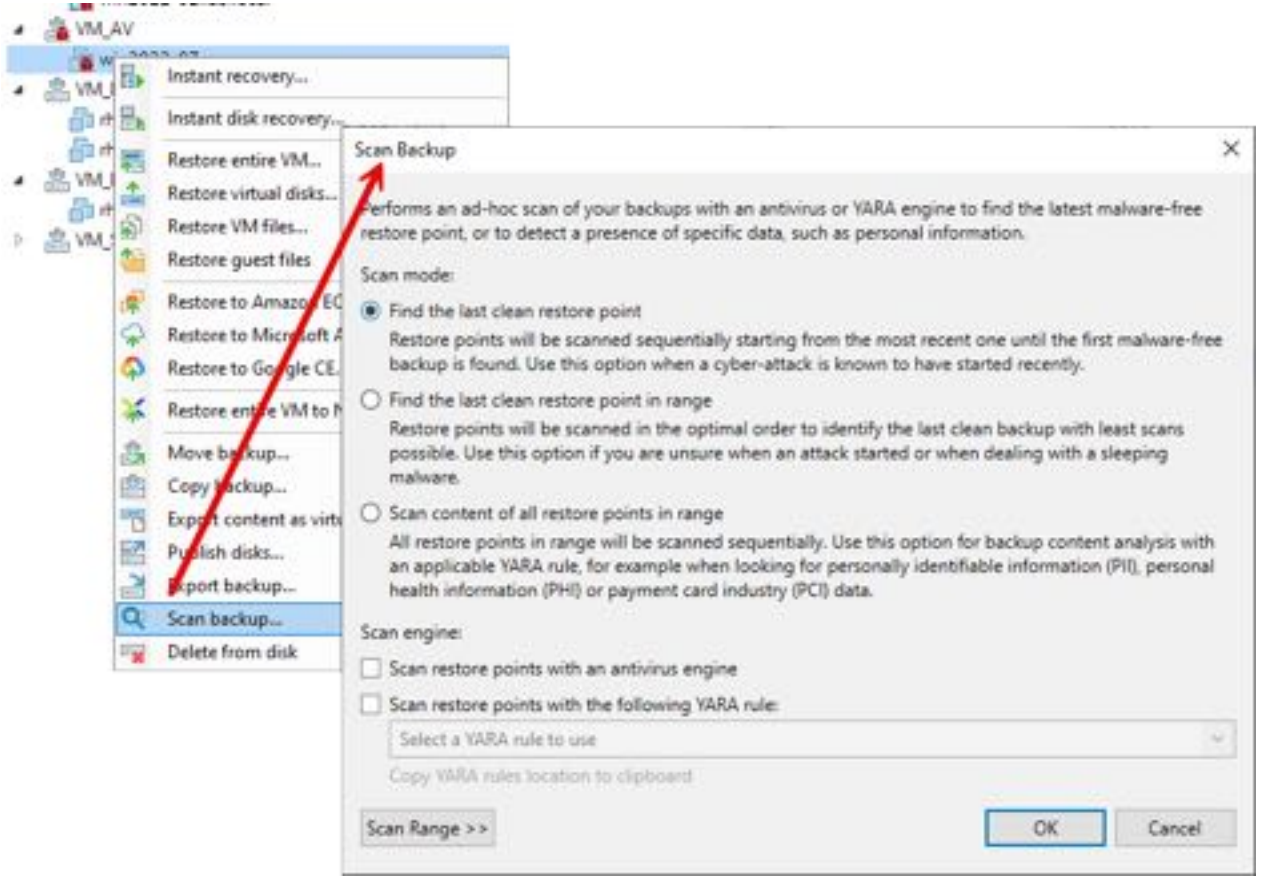
- AV und YARA Scan (Mount Server)
- What is YARA (Yet Another Ridiculous Acronym)?
  - Tool zum Aufspüren von Schadsoftware
  - Community ist fleißig
  - Jeder kann Regeln schreiben



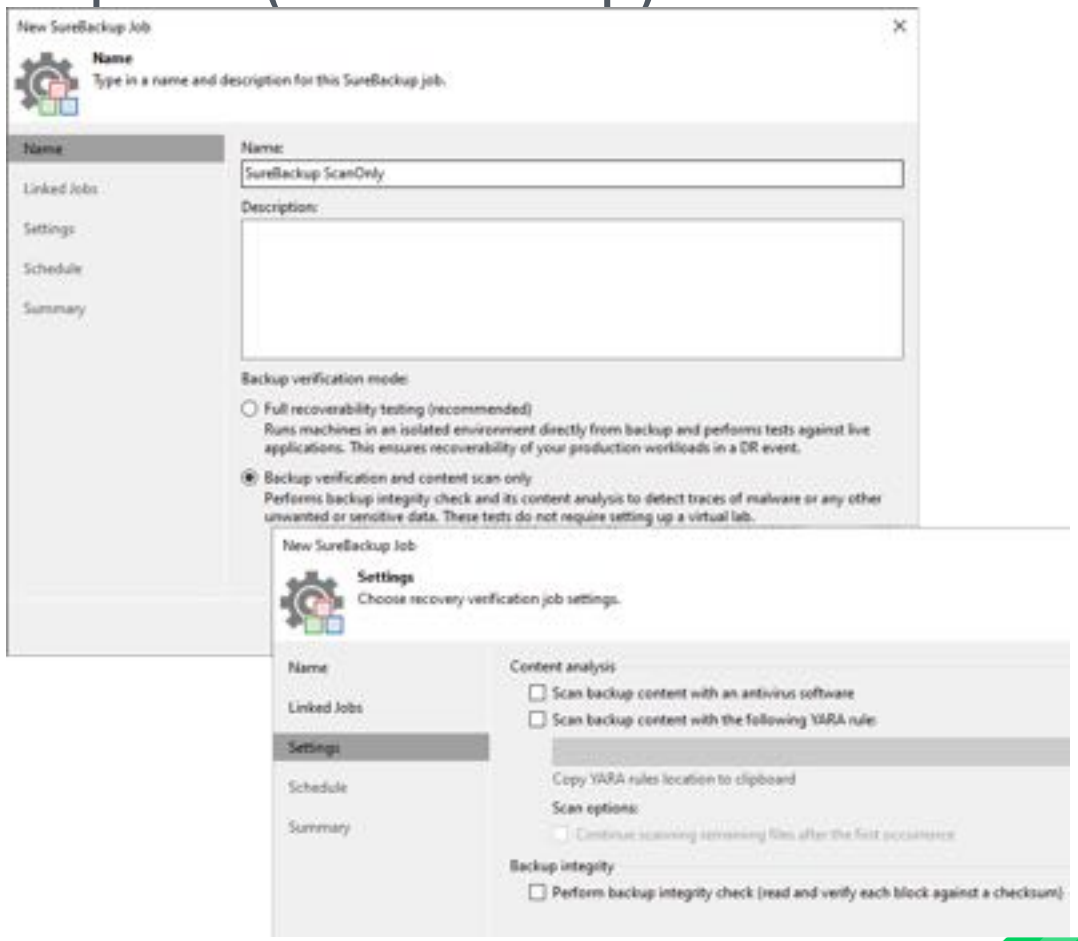
Malware Detection Methoden

On Demand Scan

Manuell



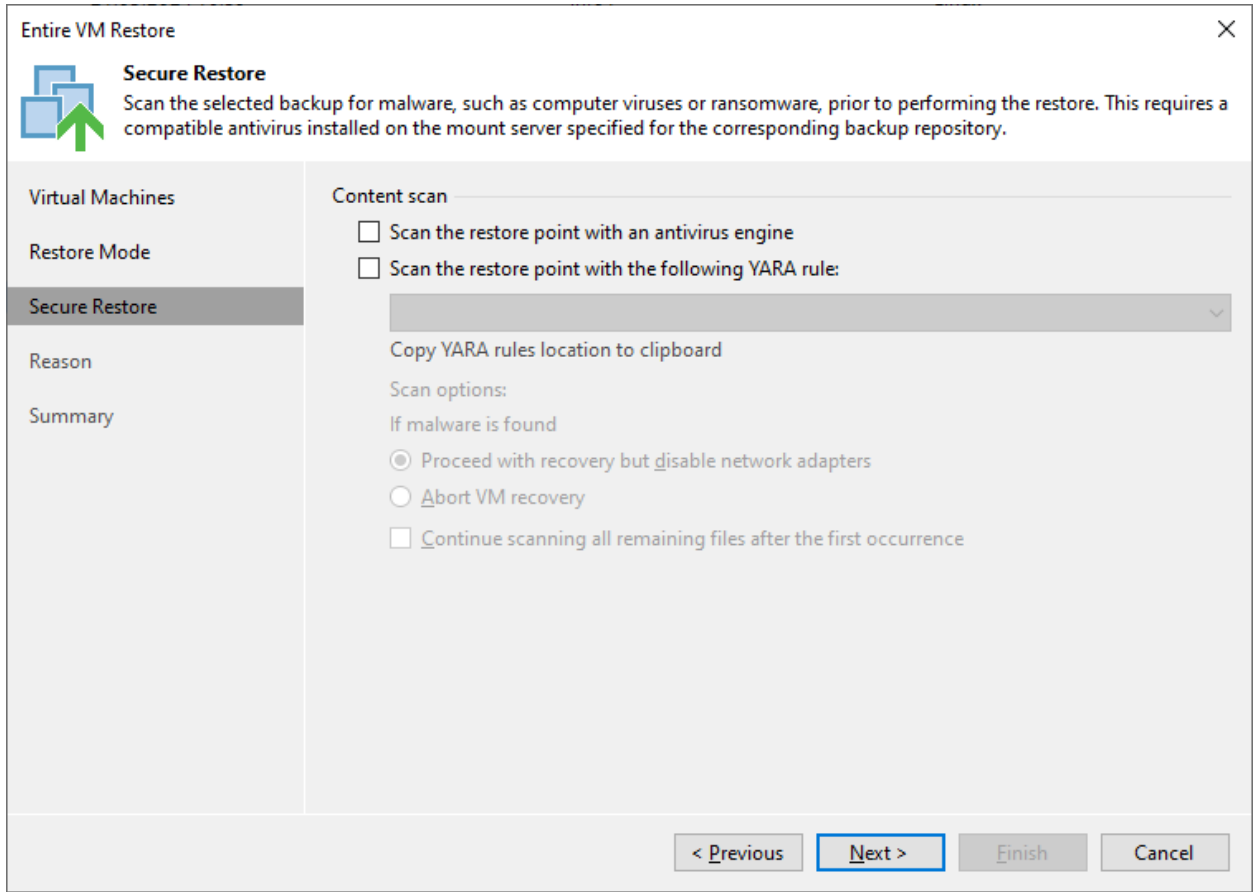
Geplant (SureBackup)



Malware Detection Methoden

On Demand Scan

und natürlich Secure Restore



Malware Detetion in Veeam ONE

Section 3

Wie kann Veeam ONE helfen

Malware Detection in Veeam ONE

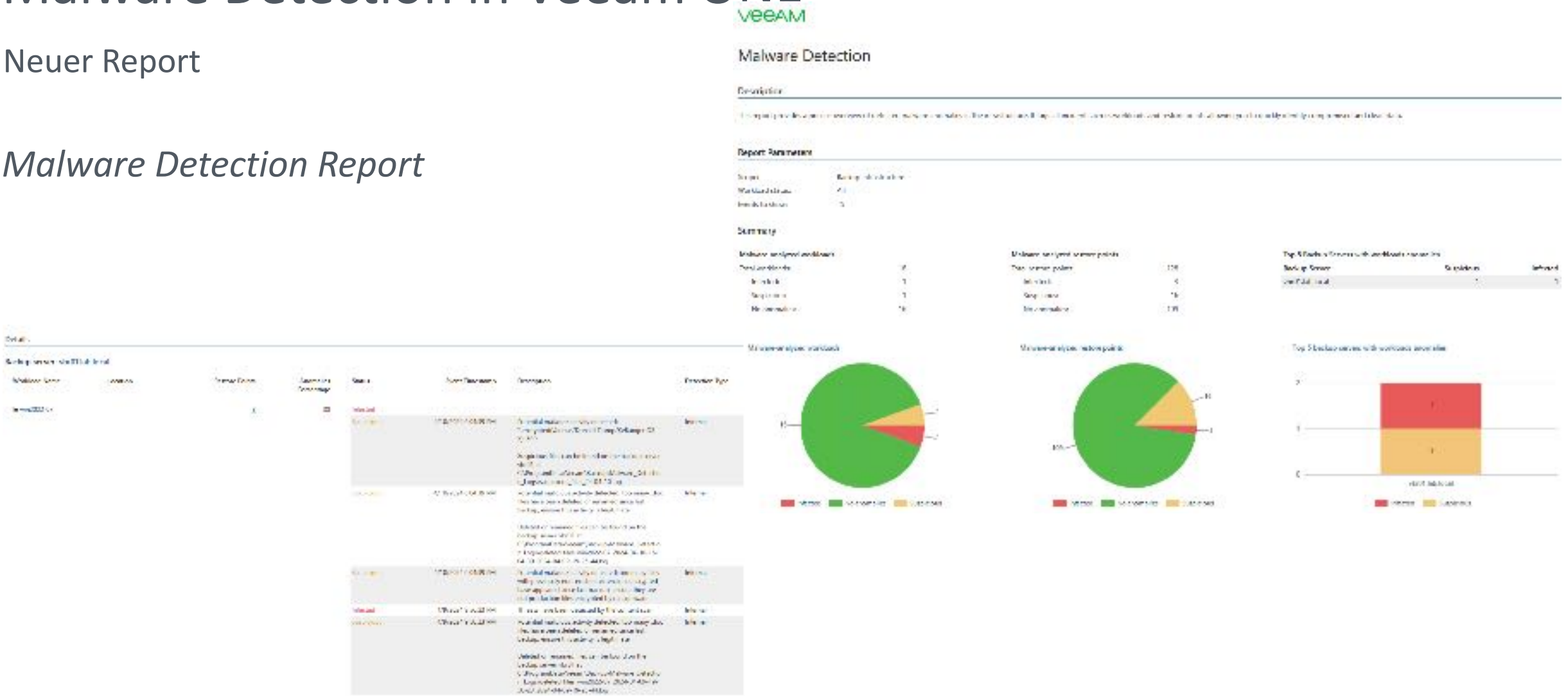
Neue Alarme

- 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



Follow us!

Join the community hub: