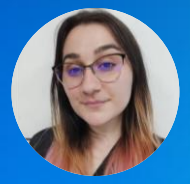
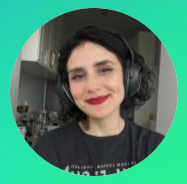
Veeam Data Platform

Sicherheits-Best Practices



Valentina Ionita

Renewals System Engineer



Diana Boro

Renewals Systems Engineer

Tagesordnung

1. Schutz der Datenschutz-Umgebung
2. Absicherung von Backups vor Verlust oder Ransomware
3. Verhinderung einer erneuten Infektion
4. Begrenzung interner Risiken
5. Reduzierung des Risikos einer weitreichenden Sicherheitsverletzung
6. Nachverfolgung beschädigter oder manipulierter Daten
7. Erweiterung der Sicherheit über Backup-Lösungen hinaus
8. Ermöglichung einer zuverlässigen und schnellen Disaster Recovery

Hinweis zu den Materialien und Ressourcen

Dieses Folienset enthält zahlreiche anklickbare Links zu verschiedenen Artikeln und weiteren Ressourcen für Ihr vertiefendes Lernen und Ihre eigene Recherche.

Eine PDF-Version des Foliensets wird Ihnen kurz nach Abschluss dieser Schulung per E-Mail zur Verfügung gestellt. Bitte halten Sie dafür Ihren Posteingang im Blick.

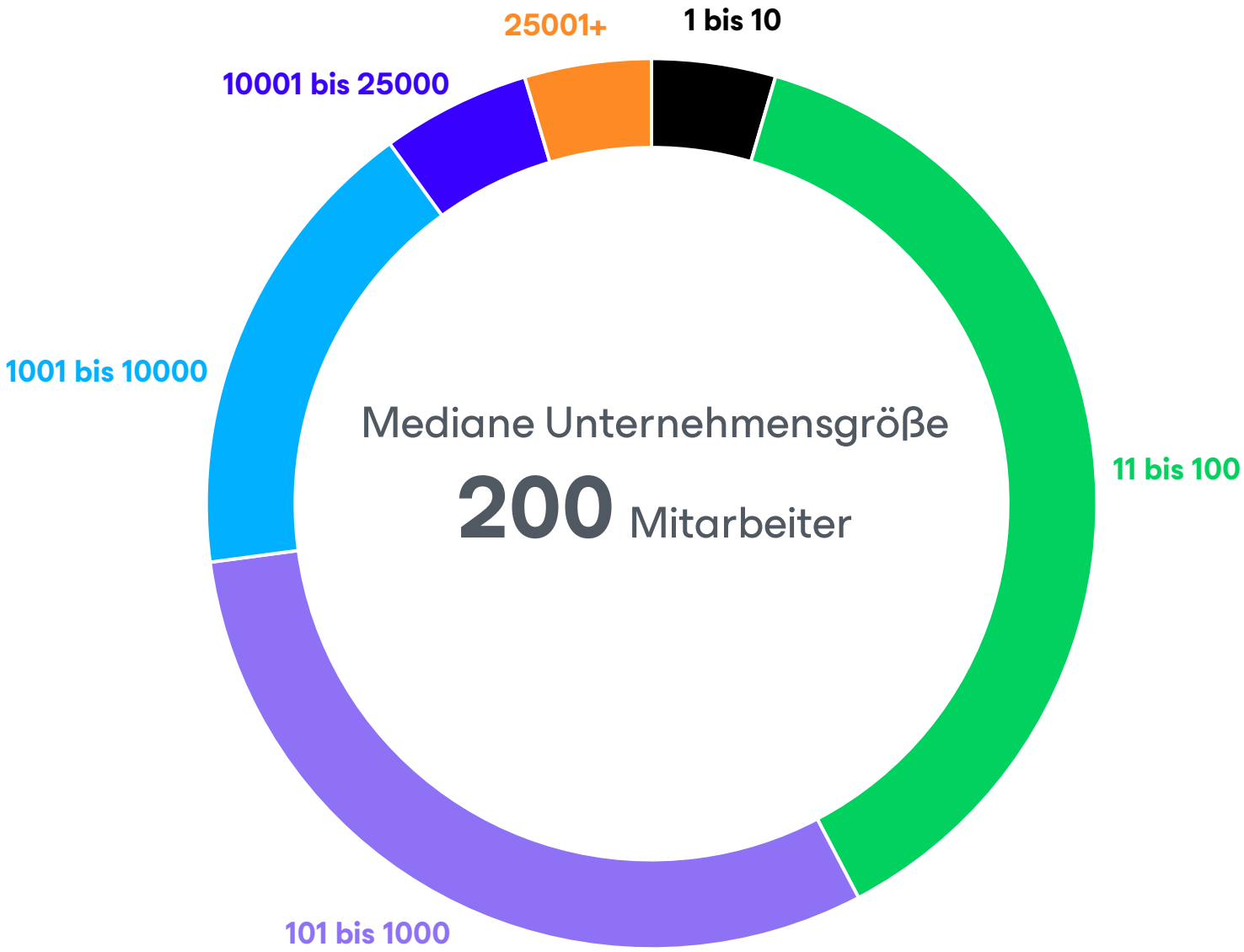
© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Die Illusion von Sicherheit

90 % der Ransomware-Opfer glaubten, vor dem Sicherheitsvorfall vorbereitet zu sein – aber nur 28 % konnten ihre Daten wiederherstellen

Angriffe können Organisationen jeder Größe treffen.

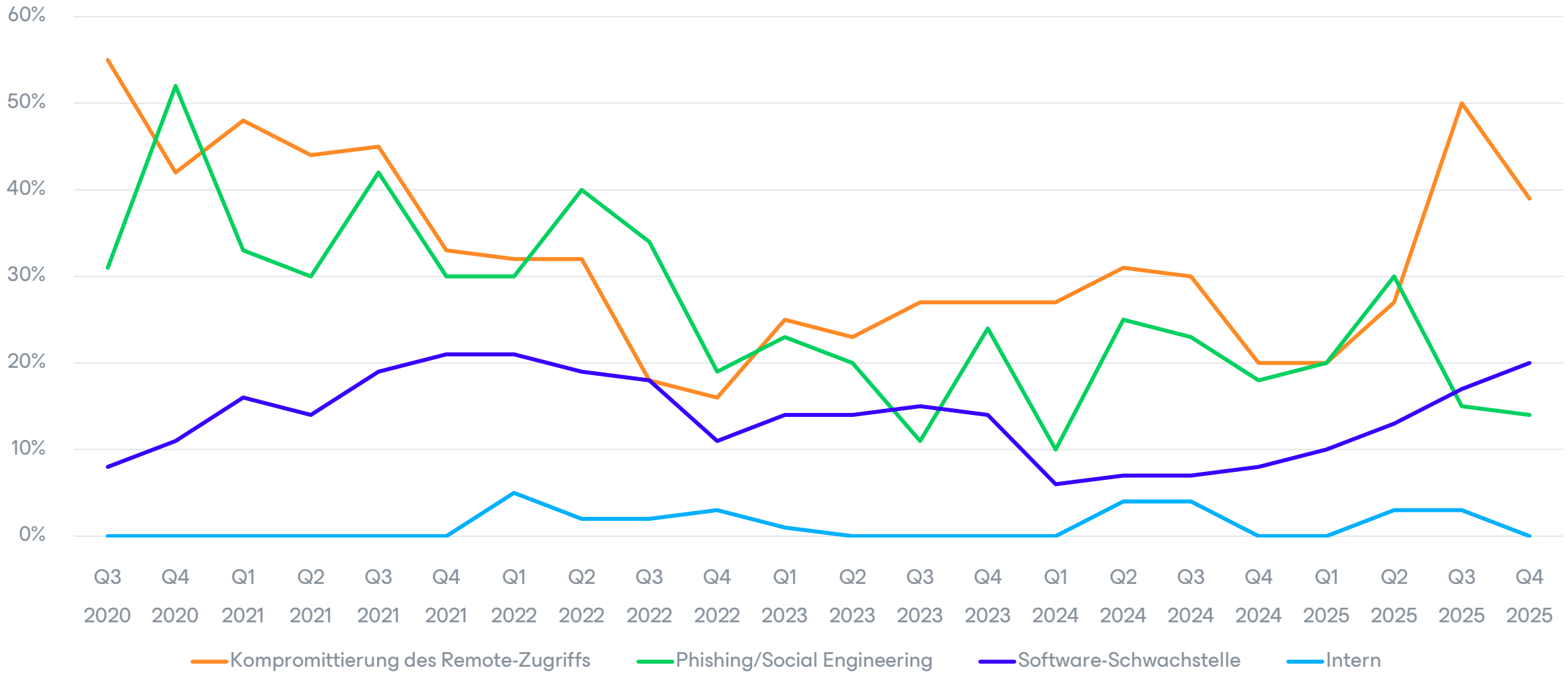
Von Ransomware betroffene Unternehmen nach Mitarbeiterzahl im 4. Quartal 2025



Quelle: https://www.coveware.com/blog/2025/4/29/the-organizational-structure-of-ransomware-threat-actor-groups-is-evolving-before-our-eyes

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Wie verschaffen sich Angreifer Zugriff?



Quelle: 2025 Ransomware Trends and Proactive Strategies by Veeam

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Vereinfachter Zeitablauf von Cyberangriffen

Aufklärung, anschließend Zugriff durch Social Engineering (Phishing usw.) und/oder Ausnutzung bekannter Schwachstellen.

Ressourcen entdecken, Berechtigungen ausweiten, Zugangsdaten erlangen, Abwehrmaßnahmen umgehen und Daten exfiltrieren.

Backupsystem kompromittieren, Backups, Snapshots und Replikate löschen, Backup-Dienste stoppen.

Spät in der Nacht an einem langen Feiertagswochenend e beginnt die Verschlüsselung.

Vor welchen Bedrohungen müssen Sie sich schützen?

Infrastruktur-Sicherheit

- Kompromittierung des Backup-Servers
- Netzwerkbasierte laterale Bewegung
- Allgemeine Umgebungs-schwachstellen

Daten-sicherheit

- Verschlüsselung/Löschung von Backupdateien
- Malware in Backups
- Datenvergiftung

Betriebs-sicherheit

- Insider-Bedrohungen
- Fehler bei Wiederherstellung und Orchestrierung

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Veeam Data Trust and Resilience Report **2026**

43 %

sagen, dass die Einführung von KI schneller voranschreitet als ihre Fähigkeit, Daten und Modelle abzusichern

40 %

sagen, dass Sicherheitsrichtlinien nicht aktualisiert wurden, um KI-spezifische Risiken zu berücksichtigen

42 %

haben nur eingeschränkte Transparenz über alle KI-Tools oder -Modelle, die im gesamten Unternehmen verwendet werden

25 %

nennen Shadow-IT und die unautorisierte Nutzung von KI-Tools als zentrales Anliegen

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Veeam Data Trust and Resilience Report **2026**

Die Vertrauenslücke

90 % der Befragten waren zuversichtlich, innerhalb der RTO wiederherstellen zu können. Nur 28 % der Ransomware-Opfer konnten ihre Daten vollständig wiederherstellen. KI vergrößert diese Lücke – die Einführung schreitet schneller voran als die Governance, und was keiner Governance unterliegt, wird nicht gesichert.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Risiko #1

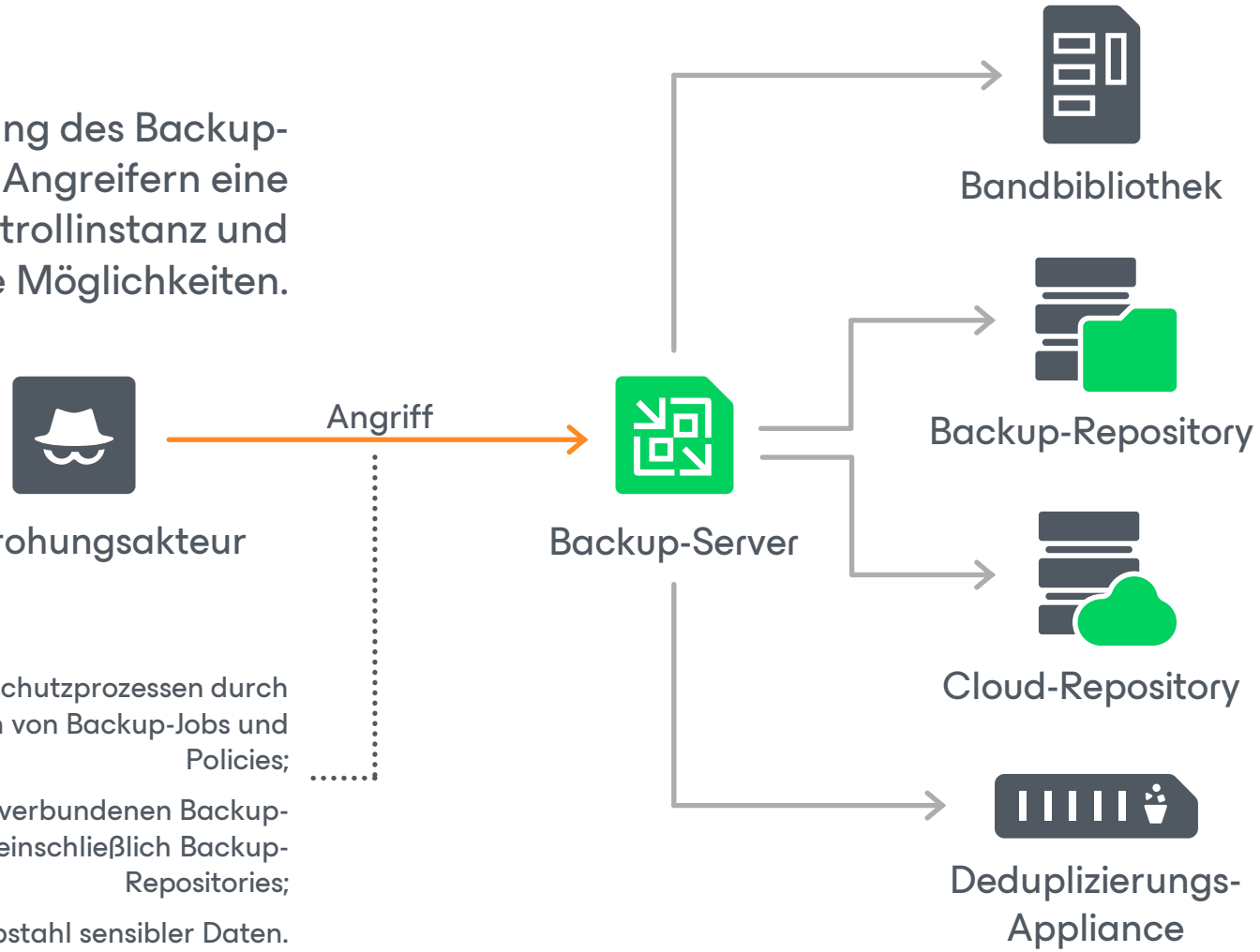
Kompromittierung des Backup-Servers

82 % der Fortune-500-Unternehmen nutzen Veeam, wodurch Backup-Server zu hochwertigen Zielen werden. Angreifer nehmen Backup-Systeme gezielt ins Visier, um eine Wiederherstellung zu verhindern.

Kompromittierung des Backup-Servers

Resilienz-Domänen

Die Kompromittierung des Backup-Servers verschafft Angreifern eine zentrale Kontrollinstanz und weitreichende destruktive Möglichkeiten.



Unterbrechen von Datenschutzprozessen durch Löschen oder Deaktivieren von Backup-Jobs und Policies;

Auffinden aller verbundenen Backup-Komponenten, einschließlich Backup-Repositories;

Diebstahl sensibler Daten.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

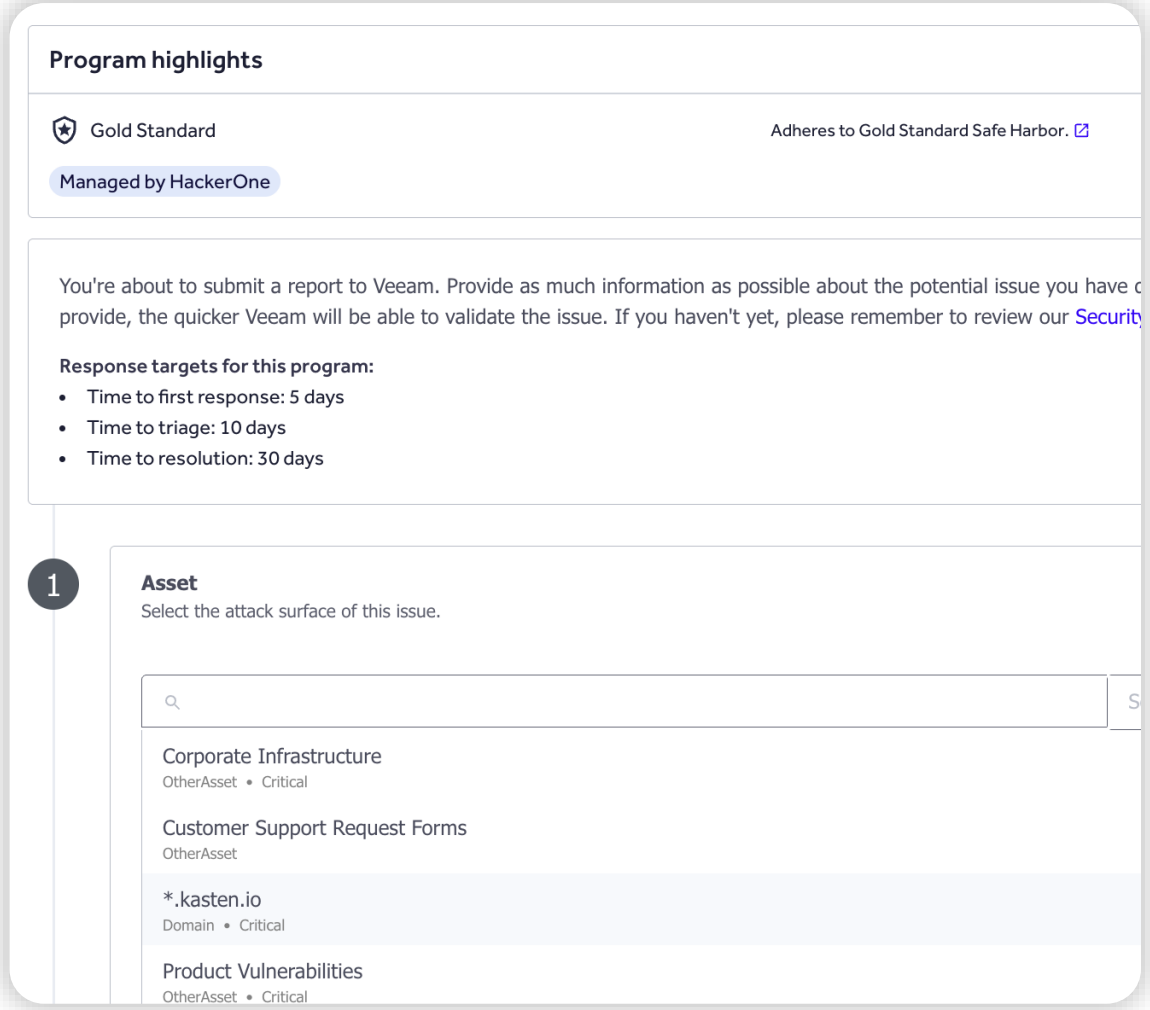
Kompromittierung des Backup-Servers

Schwachstellen in Veeam-Produkten

Bei Veeam nehmen wir Software-Schwachstellen in unseren Produkten sehr ernst.

Wir testen unsere Produkte nicht nur, sondern führen Scans und Audits durch und laden über unser öffentliches Vulnerability-Disclosure-Programm jeden dazu ein, Probleme direkt zu melden.

Wir verpflichten uns zu zeitnahen Updates, klarer Kommunikation und kontinuierlicher Verbesserung.



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

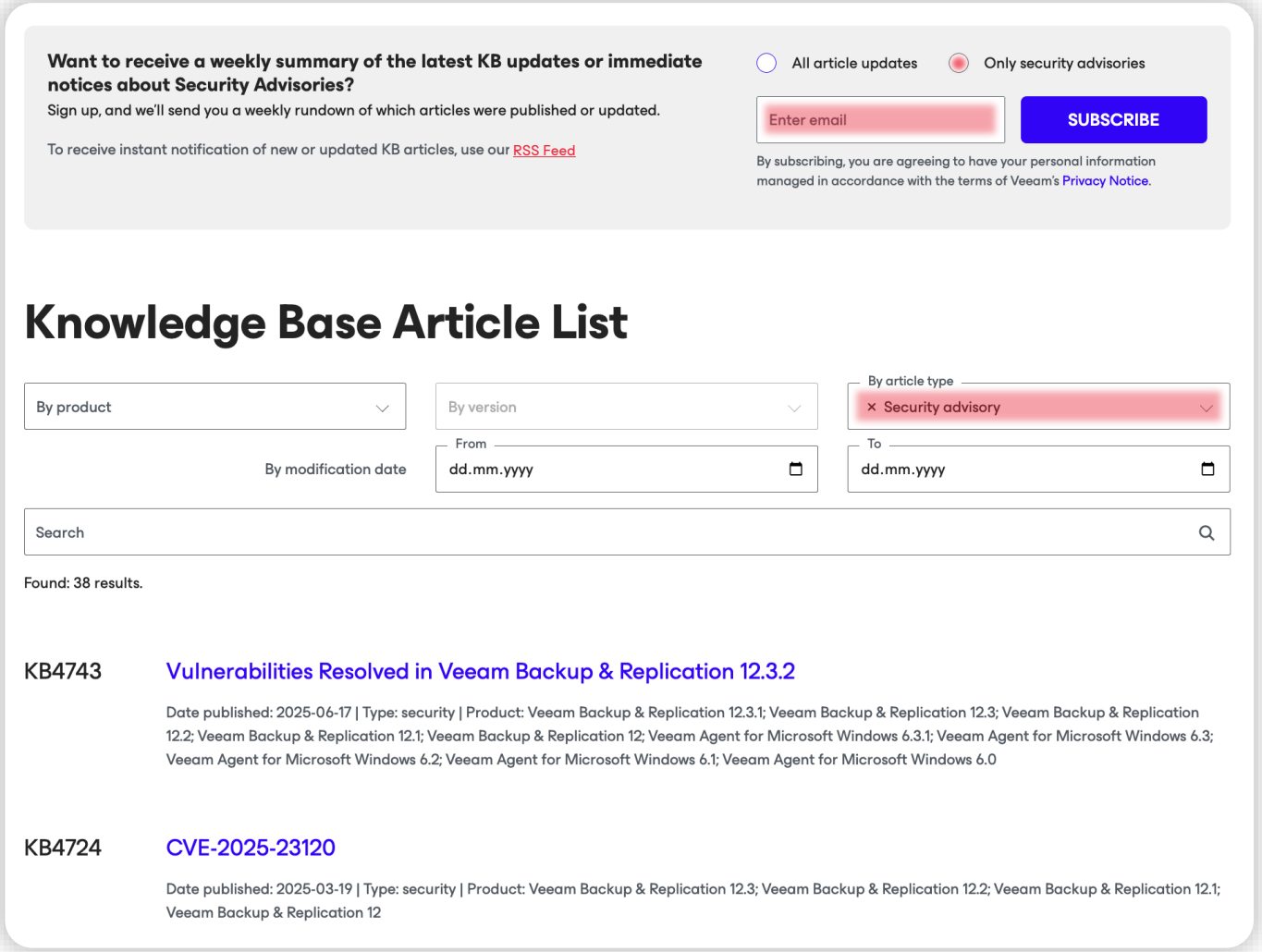
Kompromittierung des Backup-Servers

Bleiben Sie auf dem Laufenden!

Schwachstellen sind ein normaler Bestandteil der Cybersecurity-Landschaft. Ihre schnelle Identifizierung und Behebung ist entscheidend für die Resilienz Ihrer Umgebung.

Es gibt eine eigene Liste mit Security Advisories, in der Sie detaillierte Informationen zu neuen Schwachstellen und kritischen Updates finden. Diese Liste wird regelmäßig aktualisiert, sobald neue Probleme oder Patches auftreten, damit Sie schnell reagieren können.

Sie können wöchentliche E-Mail-Zusammenfassungen neuer und aktualisierter Security Advisories abonnieren oder den RSS-Feed für sofortige Benachrichtigungen nutzen.

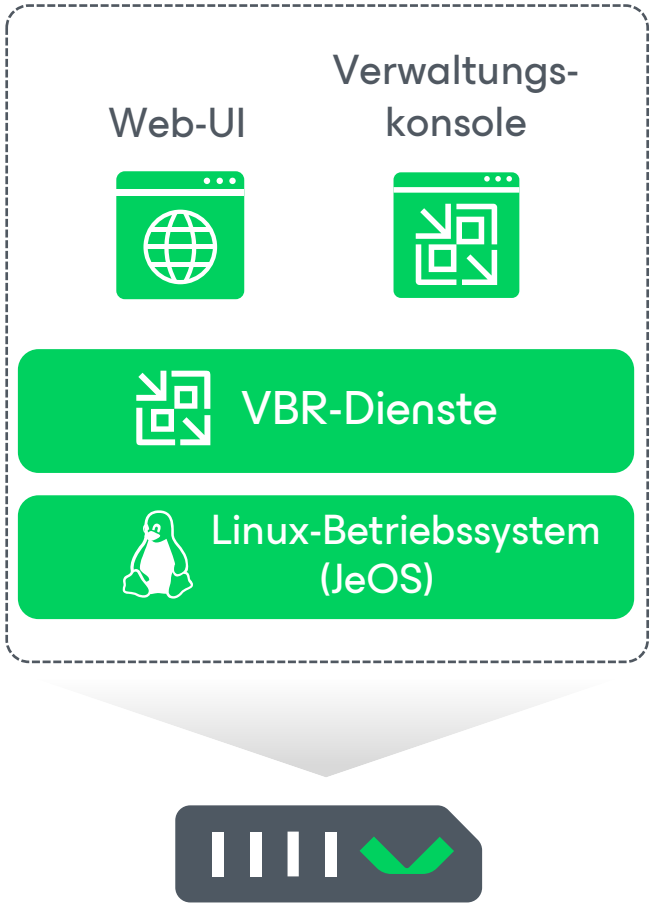


© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Kompromittierung des Backup-Servers

Veeam Software Appliance (VSA) – Sicherheitsvorteile

- **Vorgehärtete Appliance:** Die Appliance wird vorinstalliert und vorgehärtet bereitgestellt und entspricht bewährten Sicherheitspraktiken
- **Von Veeam verwaltetes Linux-Betriebssystem (JeOS):** Gemäß DIGA-STIG-Richtlinien gehärtet, mit reduzierter Angriffsfläche.
- **Integrierte Unveränderlichkeit und Zero-Trust-Kontrollen:** Implementiert Zero Trust standardmäßig
- **Automatisiertes Patching mit Veeam Updater:** Versionskontrolliert und von Veeam gepflegt
- **Starke Zugriffs-Governance:** Bietet fein abgestufte rollenbasierte Zugriffskontrolle (RBAC) und SAML-basiertes Single Sign-on für die Integration von Unternehmensidentitäten



Kompromittierung des Backup-Servers

Security & Compliance Analyzer

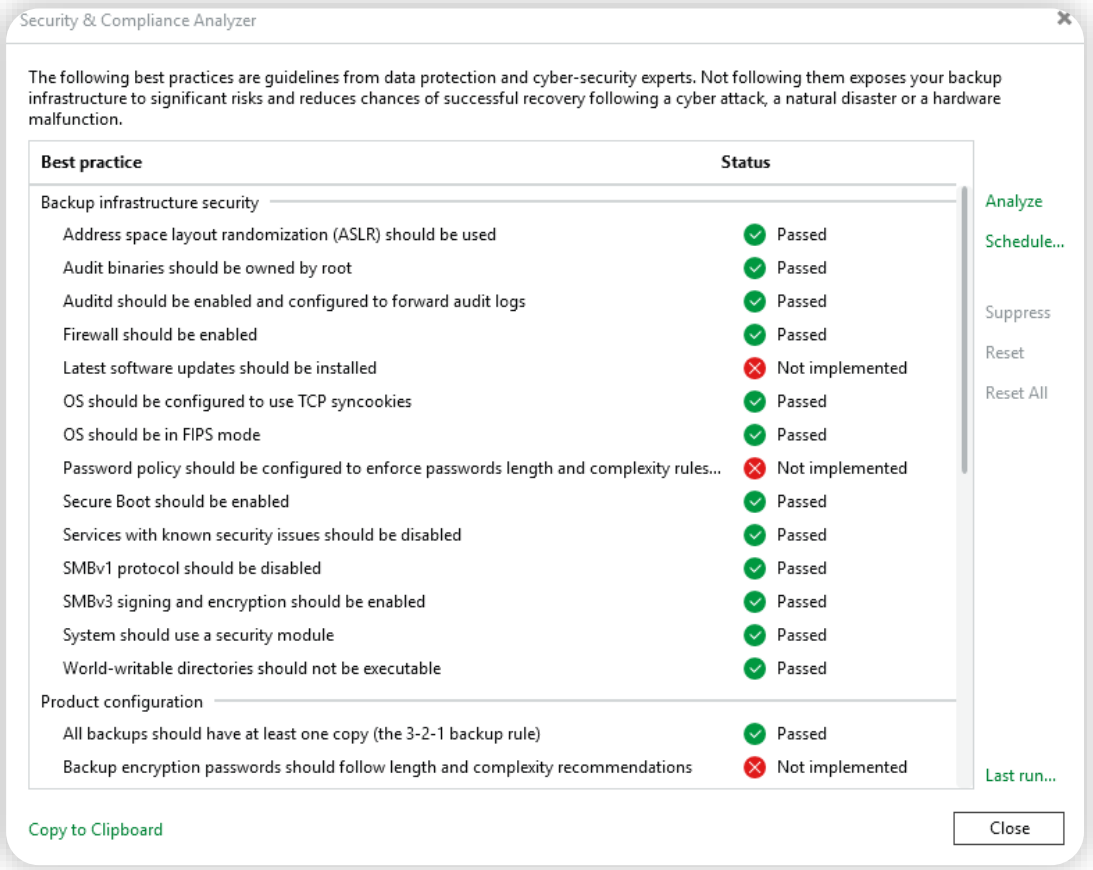
Security & Compliance Analyzer ist eine integrierte Funktion in Veeam Backup & Replication.

Dies ist ein guter Ausgangspunkt, um Ihre Umgebung zu härten.

Durch das Scannen Ihrer Umgebung auf Sicherheitsrisiken und Compliance-Lücken bietet das Tool umsetzbare Empfehlungen, um die Resilienz zu verbessern und regulatorische Anforderungen zu erfüllen.

Das Veeam Help Center stellt eine detaillierte Beschreibung zu jeder Empfehlung bereit.

Außerdem gibt es ein PowerShell-Skript (KB4525), mit dem die Umsetzung der Empfehlungen automatisiert werden kann.



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Kompromittierung des Backup-Servers

Security & Compliance Analyzer

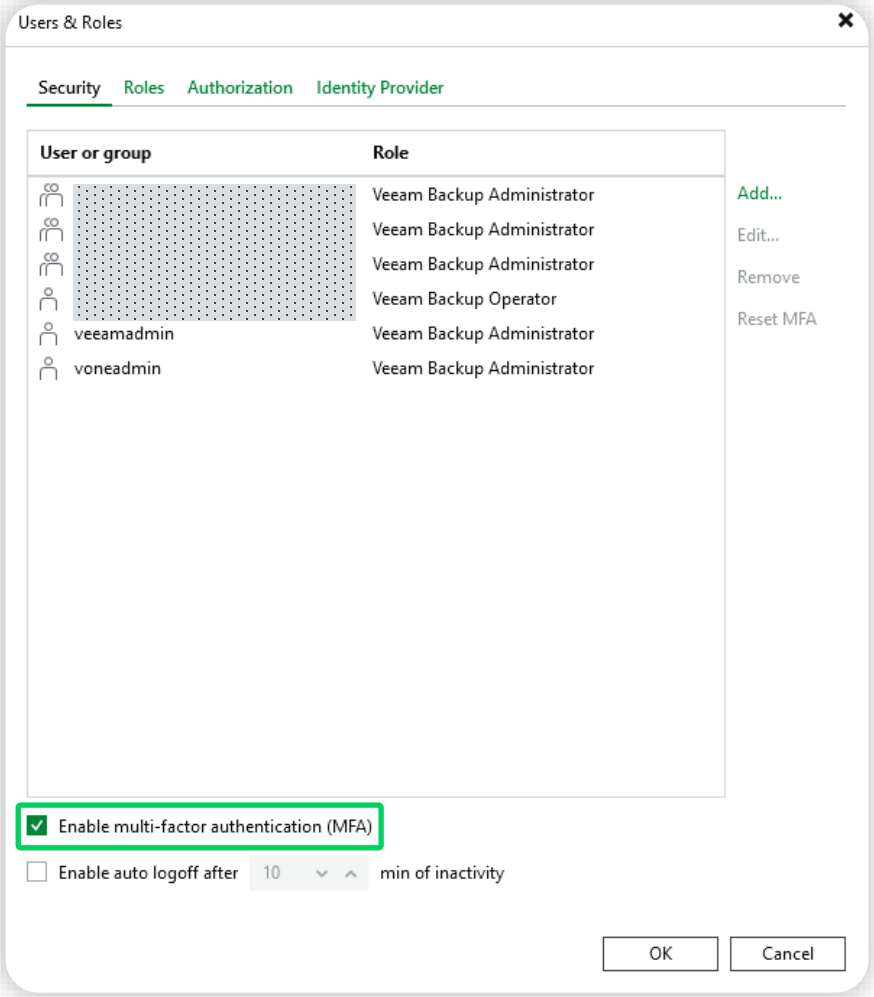
Hier sind einige der wirkungsvollsten Empfehlungen zur Härtung von Backup-Servern:

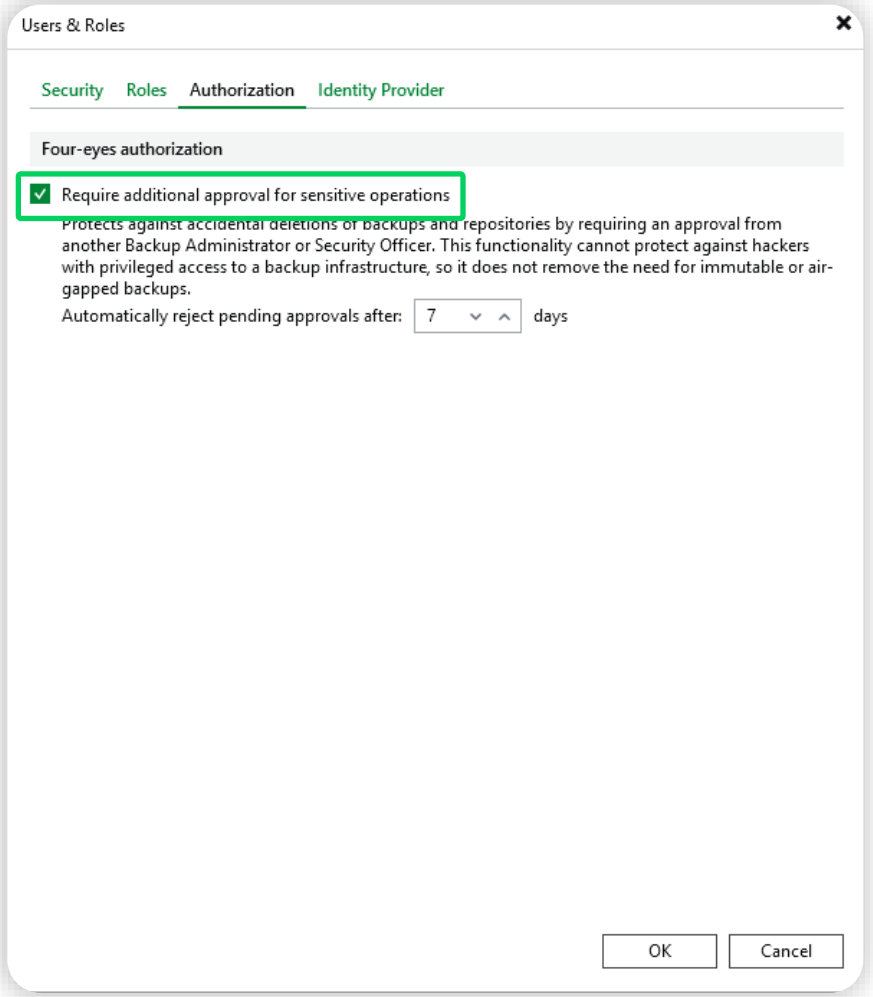
- Stellen Sie sicher, dass der Veeam Backup & Replication (VBR)-Server nicht Teil einer Active-Directory-Domäne ist. Der Betrieb des VBR-Servers in einer Arbeitsgruppe reduziert die Angriffsfläche und begrenzt laterale Bewegungen, falls Domänen-Anmeldedaten kompromittiert werden.
- Erzwingen Sie MFA für den Zugriff auf die VBR-Konsole. Dies erhöht den Schutz vor unautorisierten Anmeldungen erheblich, selbst wenn Konto-Anmeldedaten gestohlen oder erraten werden.
- Aktivieren Sie die Vier-Augen-Autorisierung, bei der zwei autorisierte Personen sensible Vorgänge genehmigen müssen.
- Verwenden Sie die Funktion „Security Officer“ (verfügbar in der Veeam Software Appliance) – eine Rolle, die Anfragen zur Zugriffserweiterung und andere sensible Vorgänge genehmigt.
- Deaktivieren Sie RDP, wo möglich, oder schränken Sie den RDP-Zugriff auf den VBR-Server stark ein. Wenn RDP erforderlich ist, beschränken Sie den Zugriff auf vertrauenswürdige IP-Adressen und verwenden Sie Authentifizierung auf Netzwerkebene, um die Exponierung gegenüber Brute-Force- und Remote-Angriffen zu reduzieren.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Kompromittierung des Backup-Servers

MFA & Vier-Augen-Autorisierung



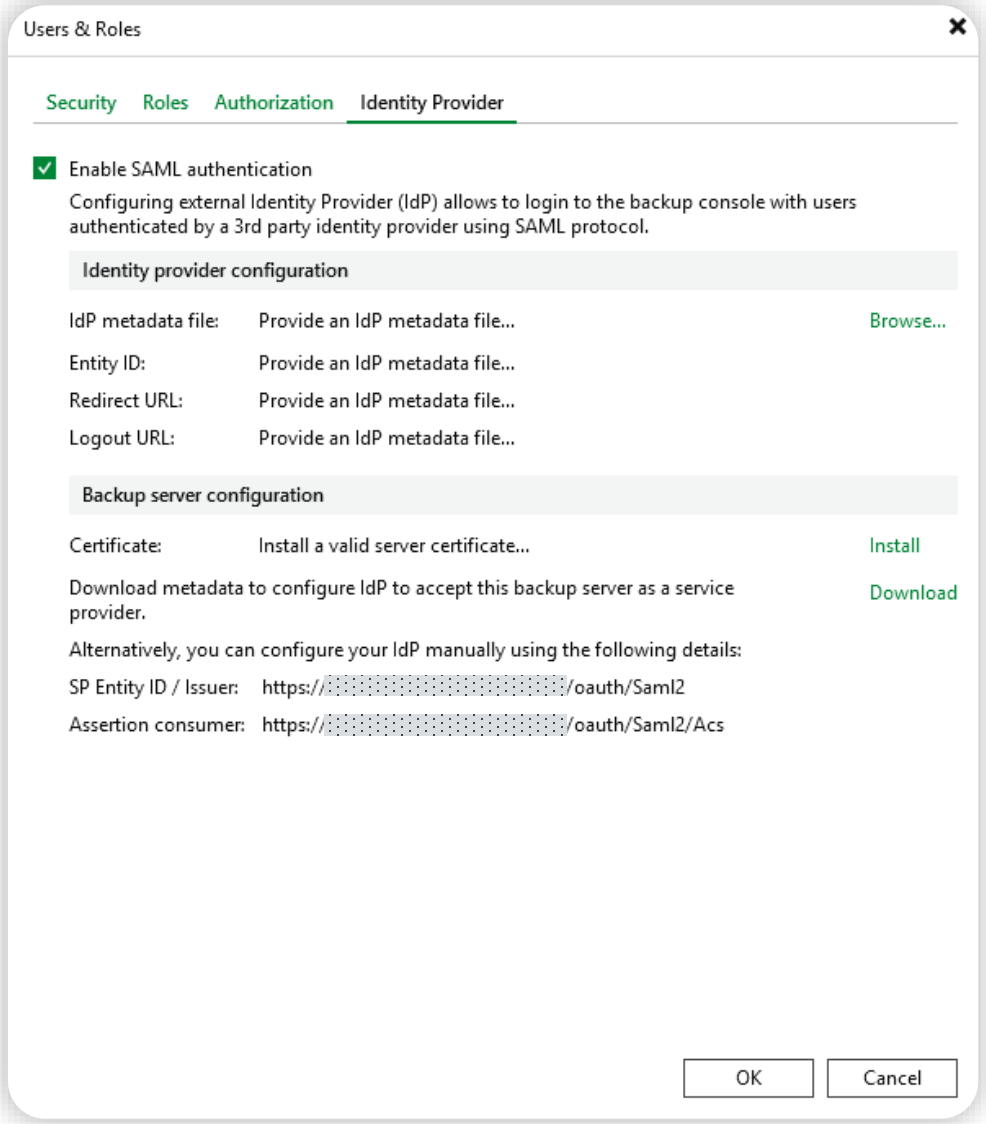


© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Kompromittierung des Backup-Servers

Identitätsanbieter

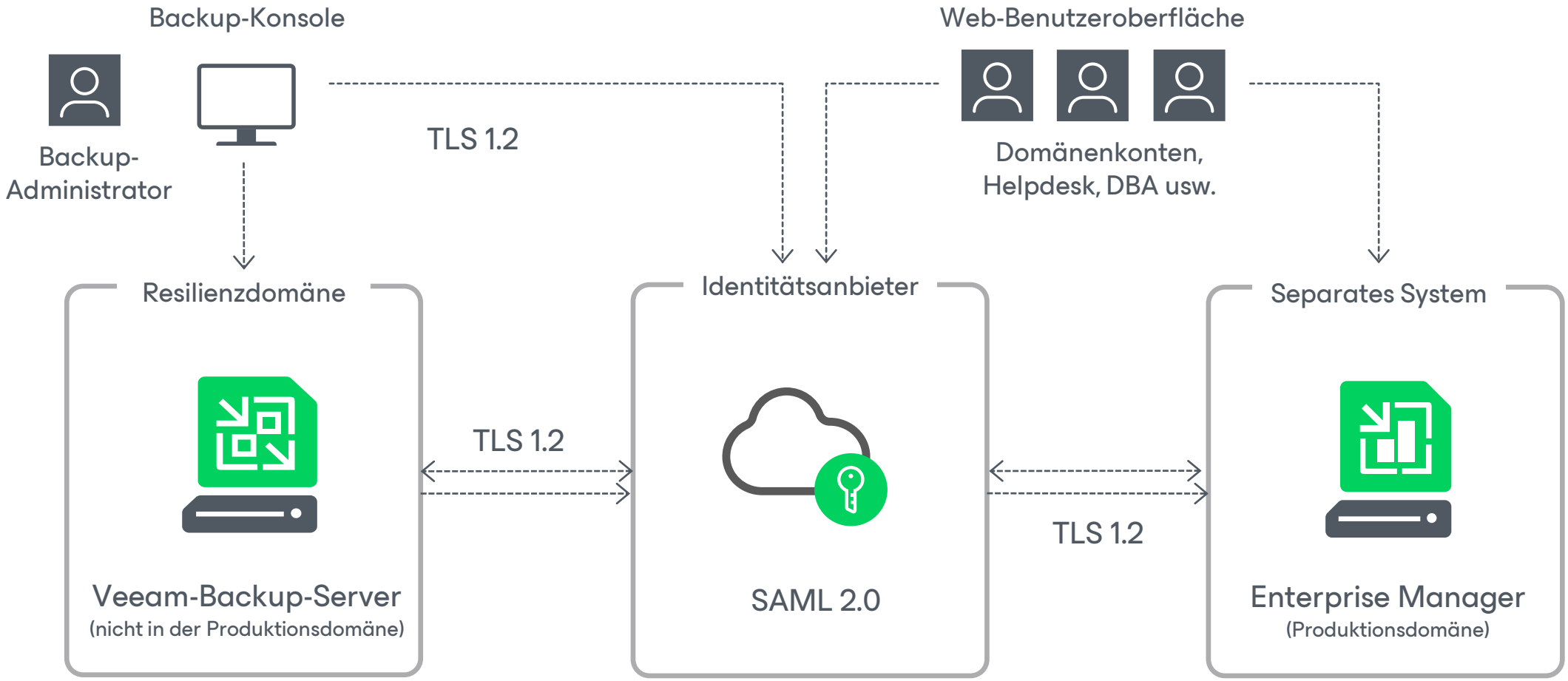
Unternehmen, die in ihrer IT-Infrastruktur einen Single-Sign-on-Dienst (SSO) verwenden, können Single-Sign-on-Funktionen auf Veeam Backup & Replication erweitern. Ein Benutzer der Organisation, der beim Single-Sign-on-Dienst angemeldet ist, kann auf Veeam Backup & Replication zugreifen, wenn sein Konto vom Veeam Backup Administrator hinzugefügt wurde.



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Rollenbasierter Zugriff

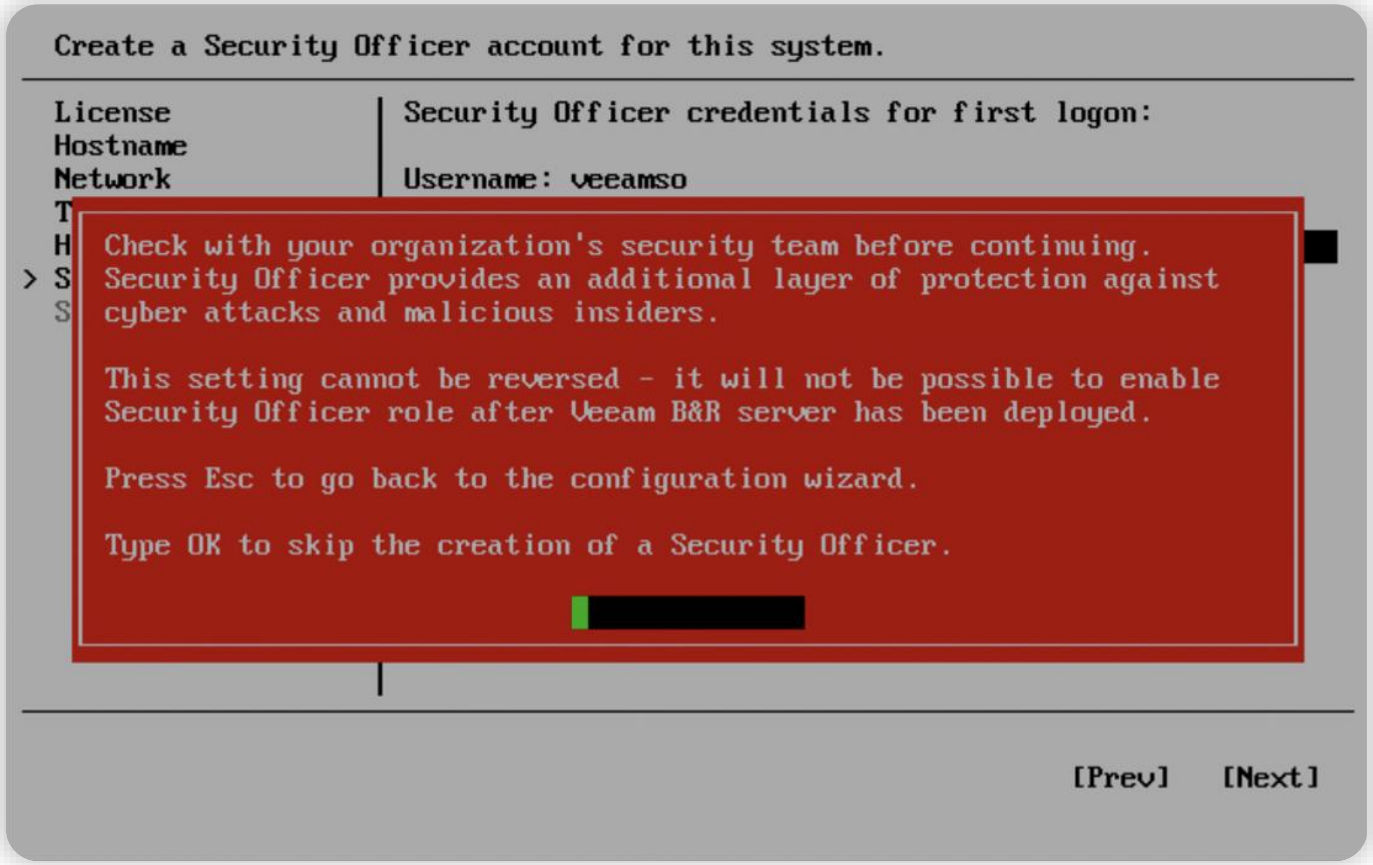
Rollenbasierte Zugriffskontrolle mit SAML-2.0-Single-Sign-on und MFA



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Kompromittierung des Backup-Servers

Security Officer (Veeam Software Appliance)



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Sicherheit hinter den Kulissen

V13-Funktionen zur Verbesserung der Sicherheit

~~RPC / WMI~~ → gRPC (plattformübergreifend)

- Weniger offene Firewall-Ports
- Bessere Leistung
- Reduzierte Netzwerkexposition

~~NTLM~~ → Kerberos

- NTLS-Schwachstellen vermeiden
- An modernen Standards ausrichten

~~OpenSSL 1.x~~ → OpenSSL 3.0

- Einhaltung von Verschlüsselungsstandards
- Resilienz gegenüber Schwachstellen
- Zukunftssicher

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

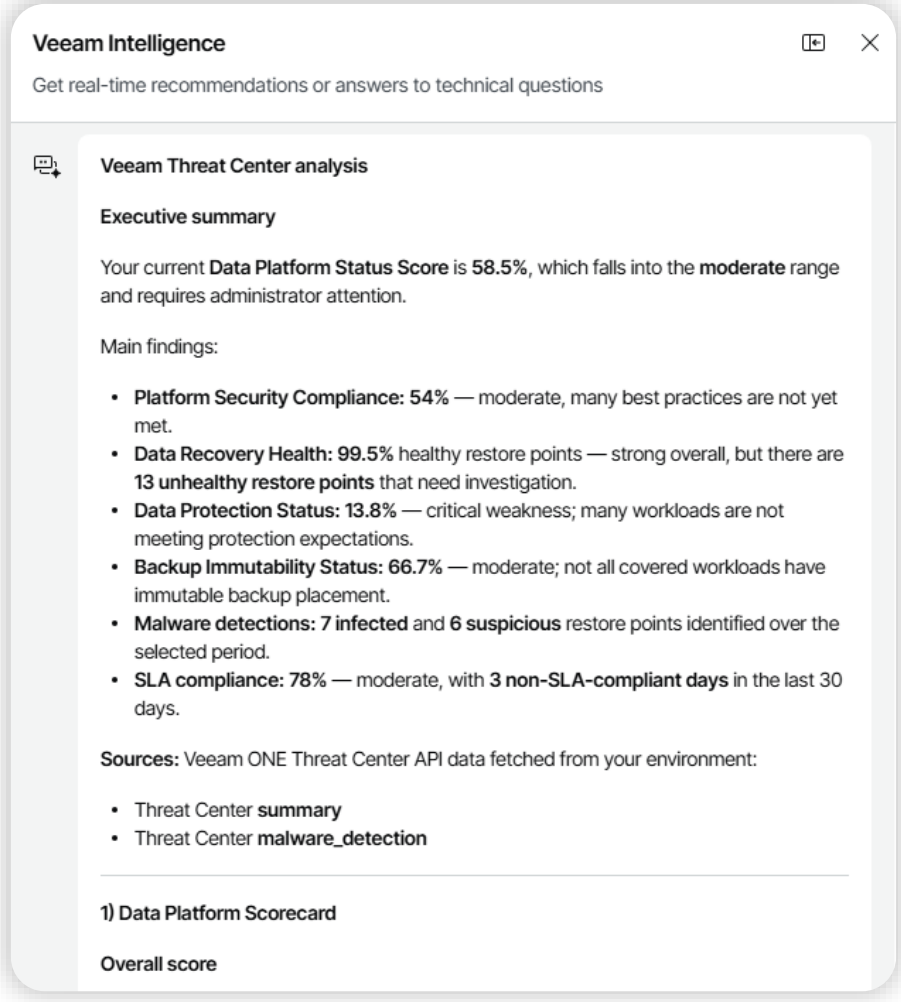
Veeam ONE: KI-gestützte Observability

Malware Deep Analysis Agent — wenn ein Alarm ausgelöst wird: fasst Anomalien zusammen, ordnet den Blast Radius pro Workload zu, identifiziert den nächstgelegenen sauberen Wiederherstellungspunkt, löst signaturbasierten Scan aus – alles aus dem Chat heraus

Abfragen in natürlicher Sprache — fragen Sie in einfacher Sprache nach Schutzstatus, Alarmen und RPO-Verletzungen; der Advanced Mode ruft Live-Daten aus Veeam ONE über die REST API ab

On-Demand-Berichtserstellung — keine Menünavigation, kein manueller Aufbau von Abfragen

+ Verbindung über MCP-KI Ihrer Wahl herstellen



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Veeam ONE: Malware- und Lückenerkennung

Alarm „Mögliche Ransomware-Aktivität“ — überwacht CPU-Auslastung, Datastore-Schreibrate und Netzwerkübertragungsrate; erkennt abnormale Muster vor der Ausbreitung

Über 340 vordefinierte Alarme — Überwachung der Unveränderlichkeit, verdächtige Aktivitäten, Konfigurationsänderungen

Proaktive Lückenerkennung — Health-Check-Alarme identifizieren Lücken in der Datenintegrität und blinde Flecken bei der Datenerfassung, bevor sie die Wiederherstellung oder Audits beeinträchtigen

Bidirektionale ServiceNow-Integration — über 300 Alarme fließen direkt in den Incident-Lifecycle ein; Nachverfolgung vom Alarm bis zum Abschluss

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Kompromittierung des Backup-Servers

Konfigurations-Backup

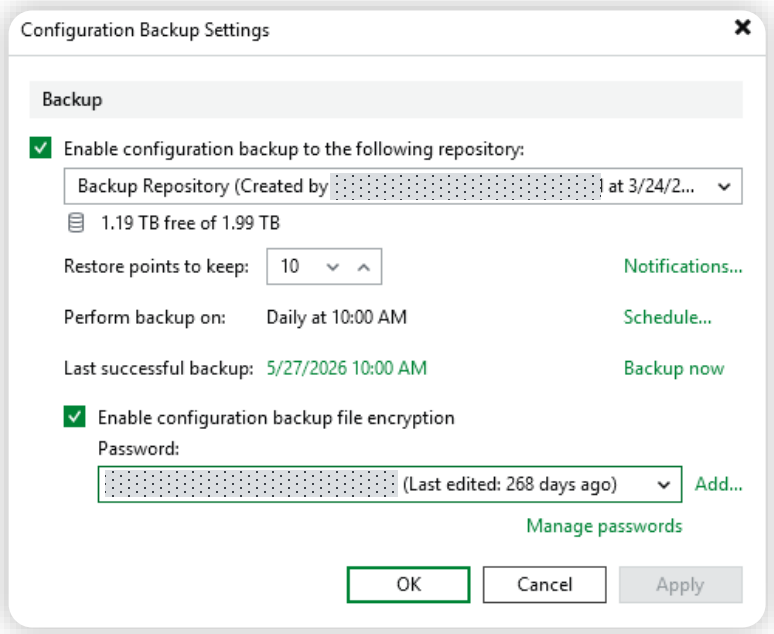
Die Sicherung der Konfigurationsdatenbank ist die Art und Weise, wie VBR „sich selbst sichert“.

Verschlüsseln Sie Daten in Konfigurationssicherungen mit dem sicheren Passwort.

Speichern Sie Konfigurationssicherungen an einem sicheren und unveränderlichen Speicherort.

Befolgen Sie das 3-2-1-Backup-Design-Framework.

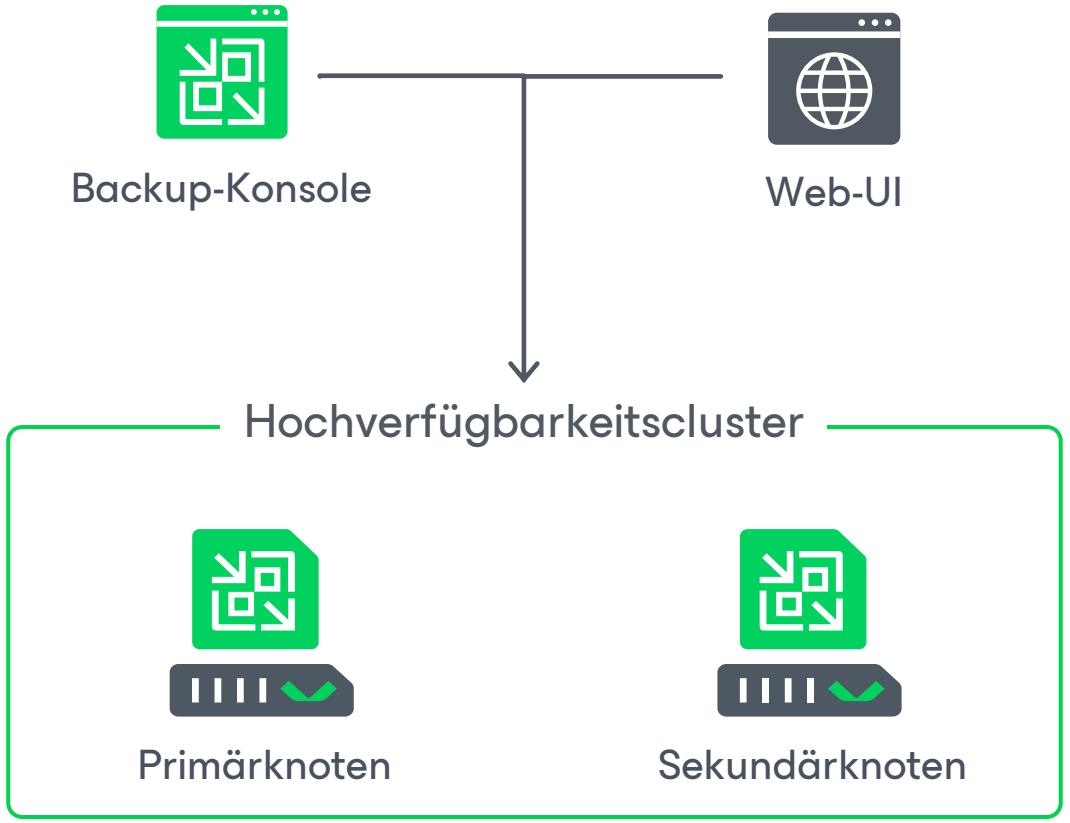
Planen Sie regelmäßige Konfigurationssicherungen, um aktuelle Wiederherstellungspunkte sicherzustellen.



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Hochverfügbarkeit

- Zwei Knoten (primär & sekundär)
- Hohe Latenz unterstützt
- Automatisierte Updates für beide Knoten
- Manuelles Failover / Knoten-Failover mit Alarm Remediation Actions (Veeam ONE) automatisieren
- Schnelle Notfallwiederherstellung ohne Konfigurationswiederherstellung



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Kompromittierung des Backup-Servers

Datenexfiltration

Datenexfiltration ist unautorisierter Datendiebstahl aus Backup- oder Produktionsumgebungen.

Angreifer exfiltrieren häufig Daten, bevor sie Ransomware einsetzen, um den Druck auf die Opfer zu erhöhen – indem sie damit drohen, gestohlene Informationen zu veröffentlichen oder zu verkaufen, wenn das Lösegeld nicht gezahlt wird. Diese Taktik erhöht nicht nur das Risiko von Datenverlust, sondern auch von Datenschutzverletzungen, Reputationsschäden und regulatorischen Strafen.

Indicators of Compromise Tools Scanner und Threat Hunter können dabei helfen, Anzeichen von Exfiltrationstools oder verdächtigen Aktivitäten zu identifizieren.

Durch die Verschlüsselung von Backups bei der Übertragung über Netzwerke und im gespeicherten Zustand stellt Veeam sicher, dass Angreifer die Daten nicht einfach lesen oder missbrauchen können, selbst wenn sie diese abfangen oder darauf zugreifen.

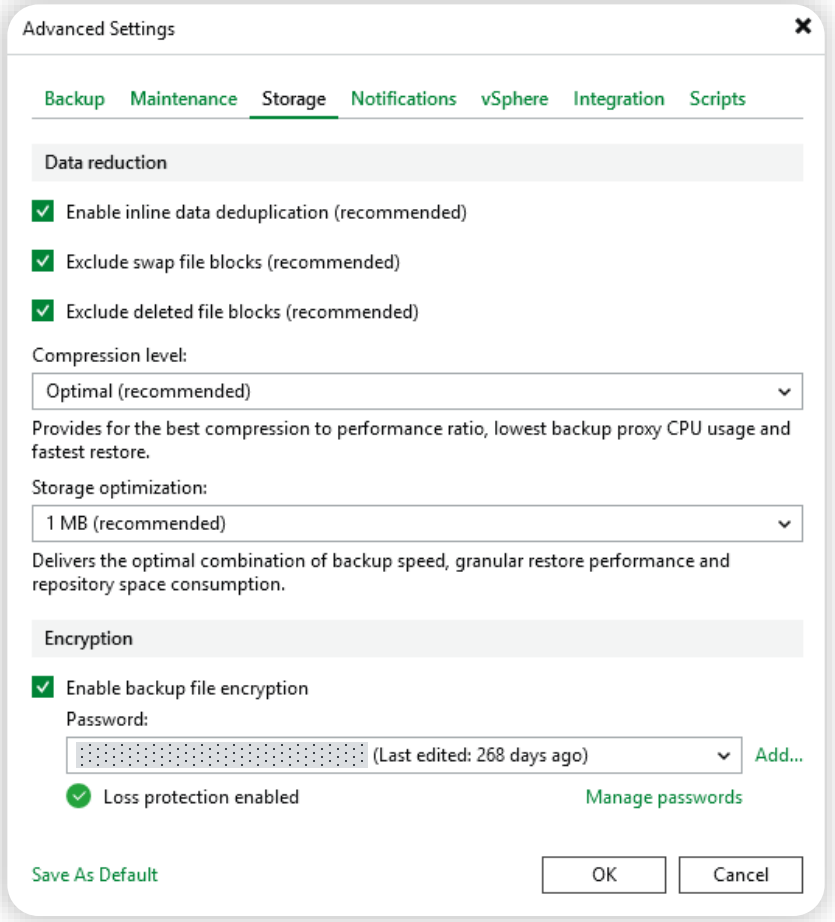
© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Verschlüsselung ist die letzte Verteidigungslinie

Wenn Angreifer Zugriff auf Backup-Dateien erhalten – ohne Verschlüsselung haben sie alles.

Daten im Ruhezustand
AES-256-CBC-Verschlüsselung auf Job-Ebene mit 256-Bit-Schlüsseln. Für Unternehmensumgebungen kann ein externes KMS Schlüssel vollständig außerhalb von VBR generieren und verwahren.

verschlüsselt auch **Daten bei der Übertragung**
Veeam verwendet TLS für die gesamte Kommunikation zwischen Komponenten. Kein unverschlüsselter Datenverkehr.



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Post-Quanten-Verschlüsselung

Veeam kombiniert bewährte AES-256-Verschlüsselung (FIPS-konform) für Backup-Daten mit Post-Quanten-Kryptografie (PQC) für Schlüsselaustausch und Systemkommunikation. Dadurch bleiben Daten heute geschützt und sind gleichzeitig auf zukünftige Quantenbedrohungen vorbereitet – ohne Auswirkungen auf bestehende Compliance-Anforderungen.

Dies ist entscheidend, da Organisationen mit „Harvest now, decrypt later“-Risiken konfrontiert sind, bei denen heute erfasste verschlüsselte Daten in Zukunft kompromittiert werden könnten. Branchenorganisationen wie NIST definieren bereits Post-Quanten-Standards und treiben damit den Bedarf an langfristiger kryptografischer Resilienz voran.

Kompromittierung des Backup-Servers

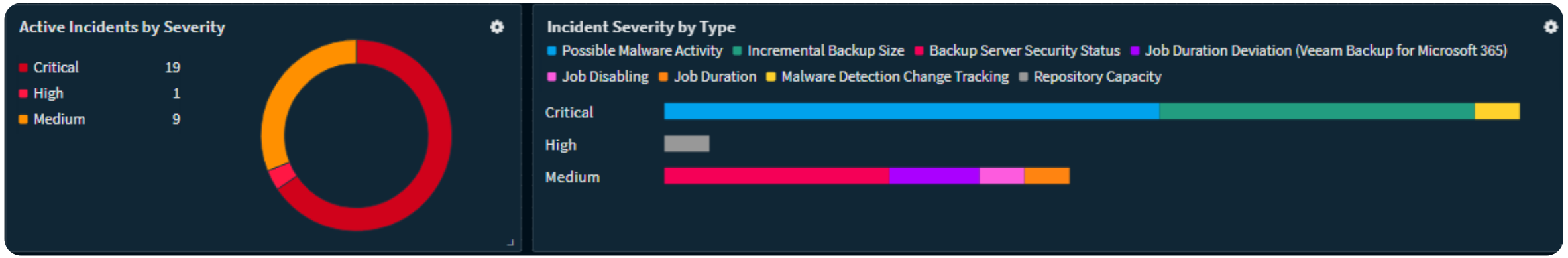
Bleiben Sie informiert: Security Information & Event Management (SIEM)

[10 kritische Alarme, um Ransomware zu stoppen und Ihre Geschäftskontinuität zu schützen]

Über 300 Ereignisse sind über die RFC-5424-Syslog-Integration verfügbar, zum Beispiel:

- Alarm bei überschrittenen MFA-Versuchen
- Alarm bei verdächtiger Ransomware-Aktivität
- Versuchte Backup-Löschungen
- Erkannte Malware-Aktivität

splunk> CROWDSTRIKE FORTINET paloalto NETWORKS SOPHOS



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

veeam

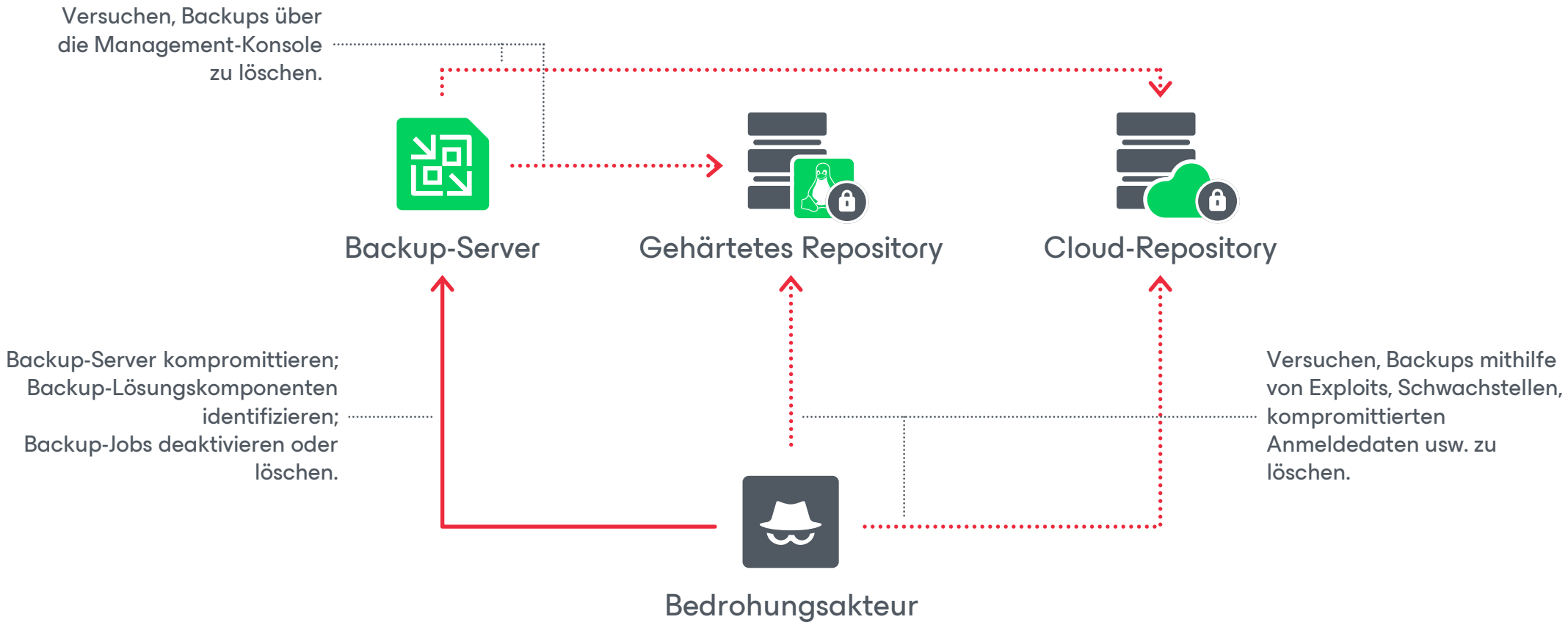
Risiko #2

Verschlüsselung/Löschung von Backup-Daten

Statistik: Bei 89 % der Organisationen wurden die Backup-Repositories ins Visier genommen, und bei mehr als einem Drittel wurden kritische Backup-Daten verändert oder zerstört.

Verhinderung der Verschlüsselung/Löschung von Backup-Daten

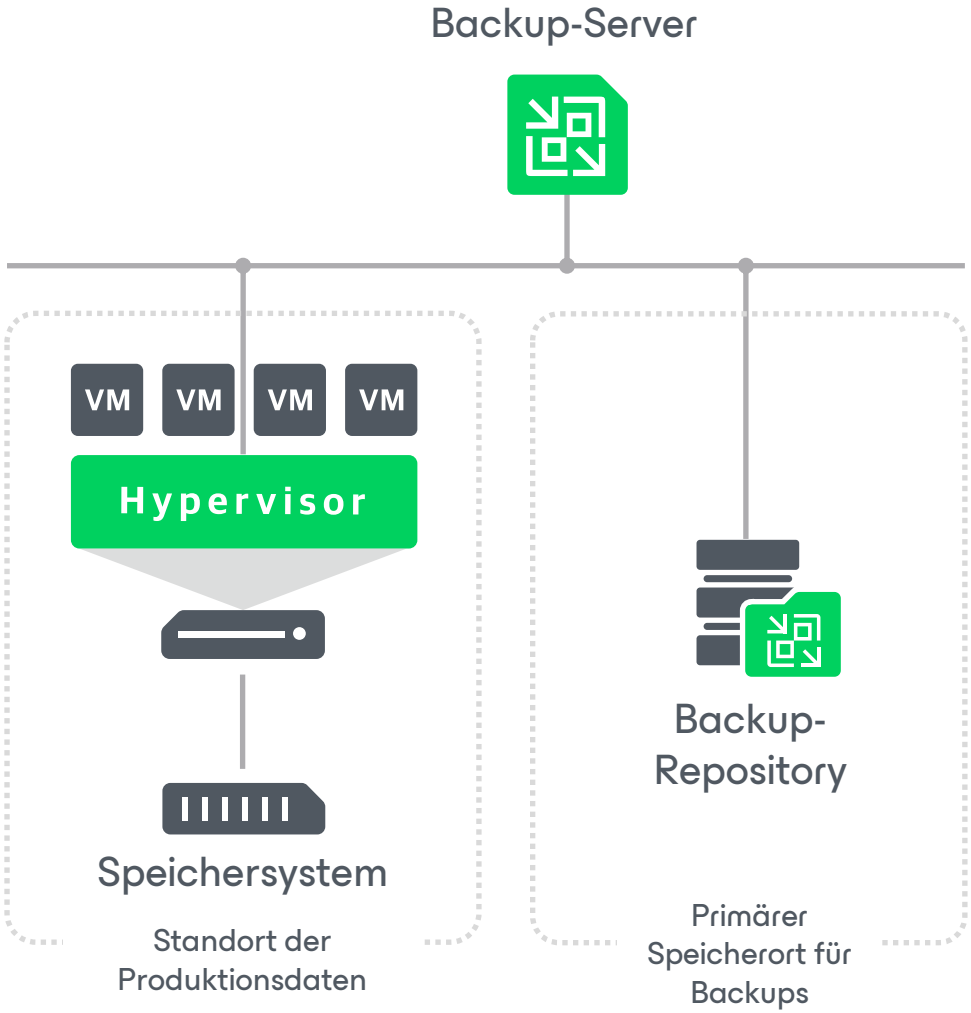
Resilienz-Domänen



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Verhinderung der Verschlüsselung/Löschung von Backup-Daten

3-2-1-Regel



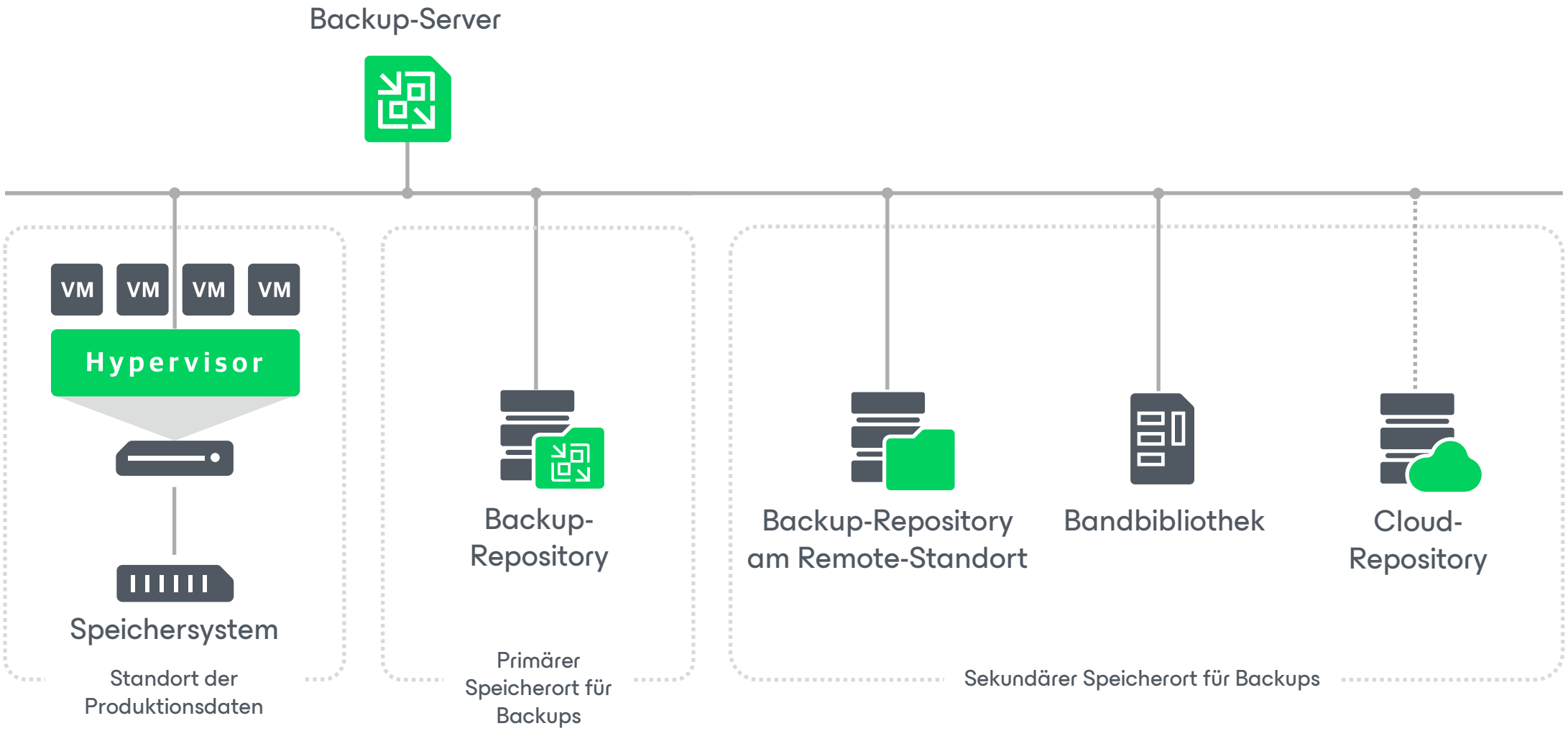
Durch das Vorhalten mehrerer Kopien auf verschiedenen Medientypen und mindestens einer externen Kopie stellt die Regel sicher, dass es keinen Single Point of Failure gibt, wodurch Datenverlust deutlich unwahrscheinlicher wird.

Wenn eine Kopie durch Hardwarefehler, menschliches Versagen oder einen Cyberangriff verloren geht, beschädigt oder kompromittiert wird, stehen Ihnen weiterhin andere Kopien zur Wiederherstellung Ihrer Informationen zur Verfügung.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Verhinderung der Verschlüsselung/Löschung von Backup-Daten

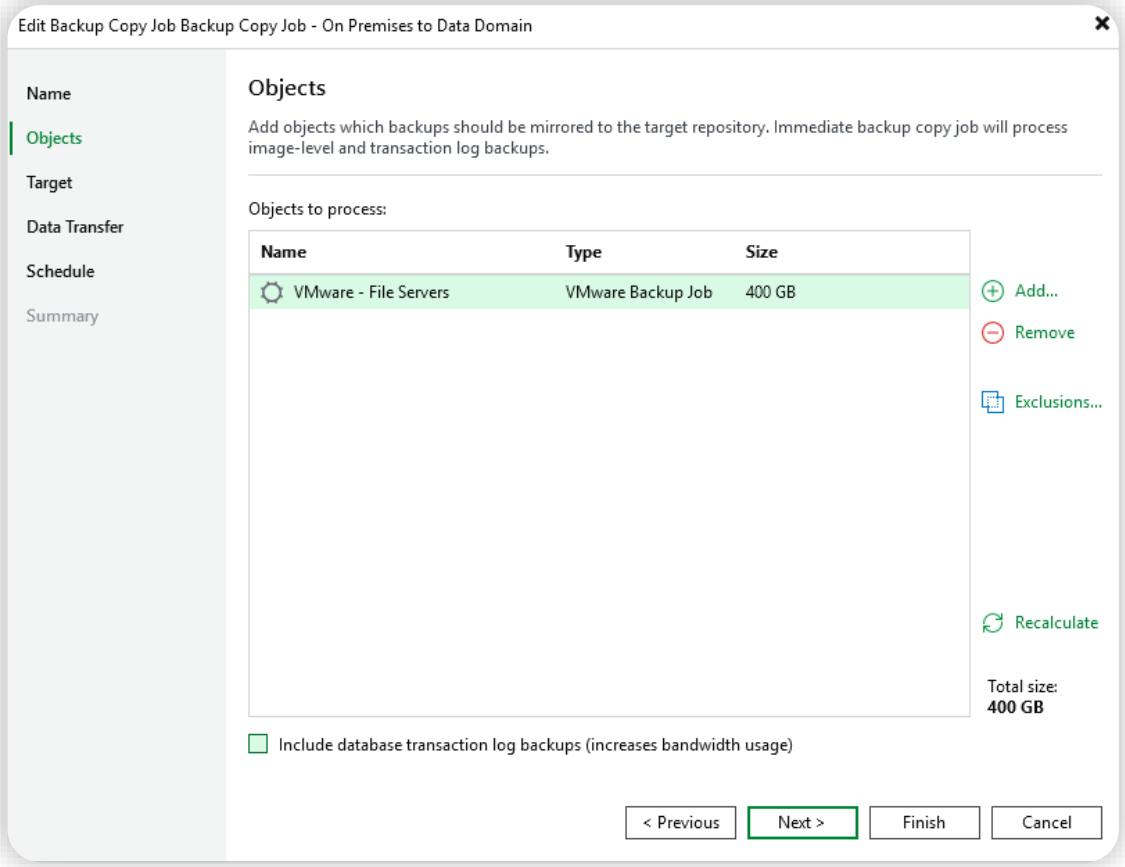
3-2-1-Regel

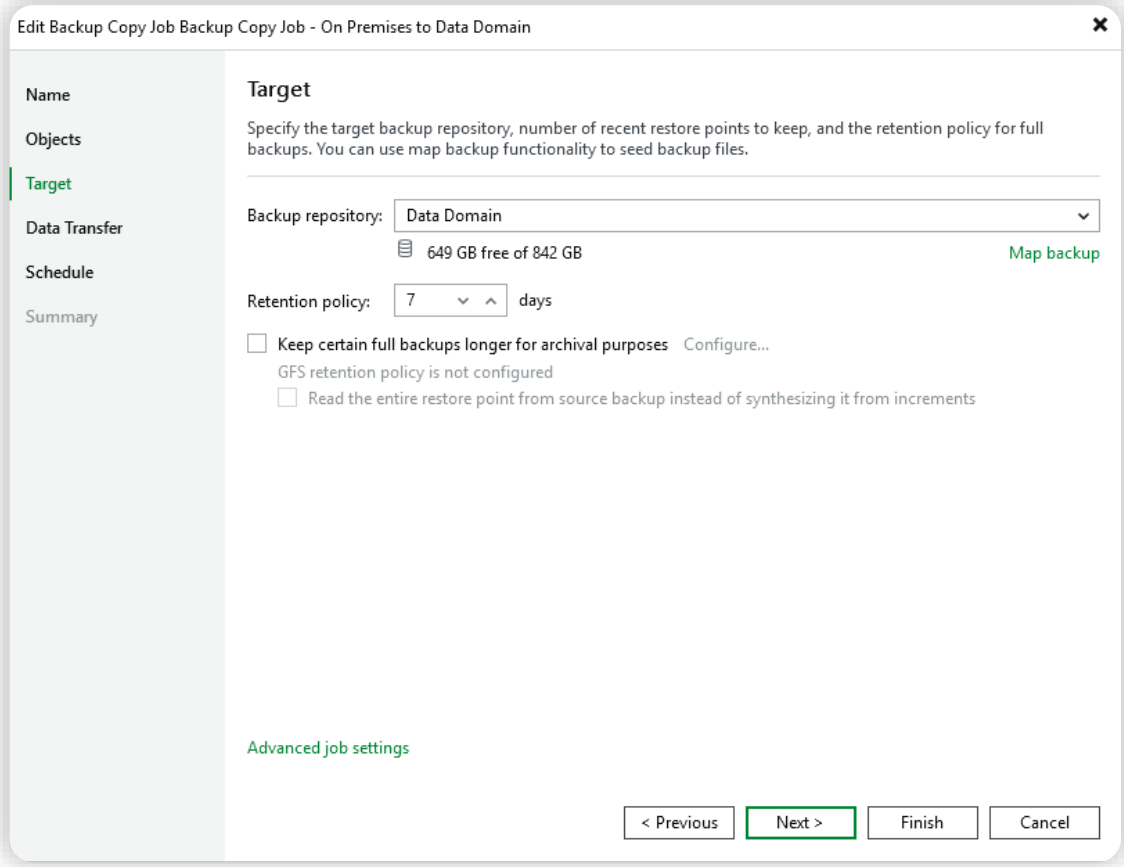


© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Verhinderung der Verschlüsselung/Löschung von Backup-Daten

Backup-Copy-Job





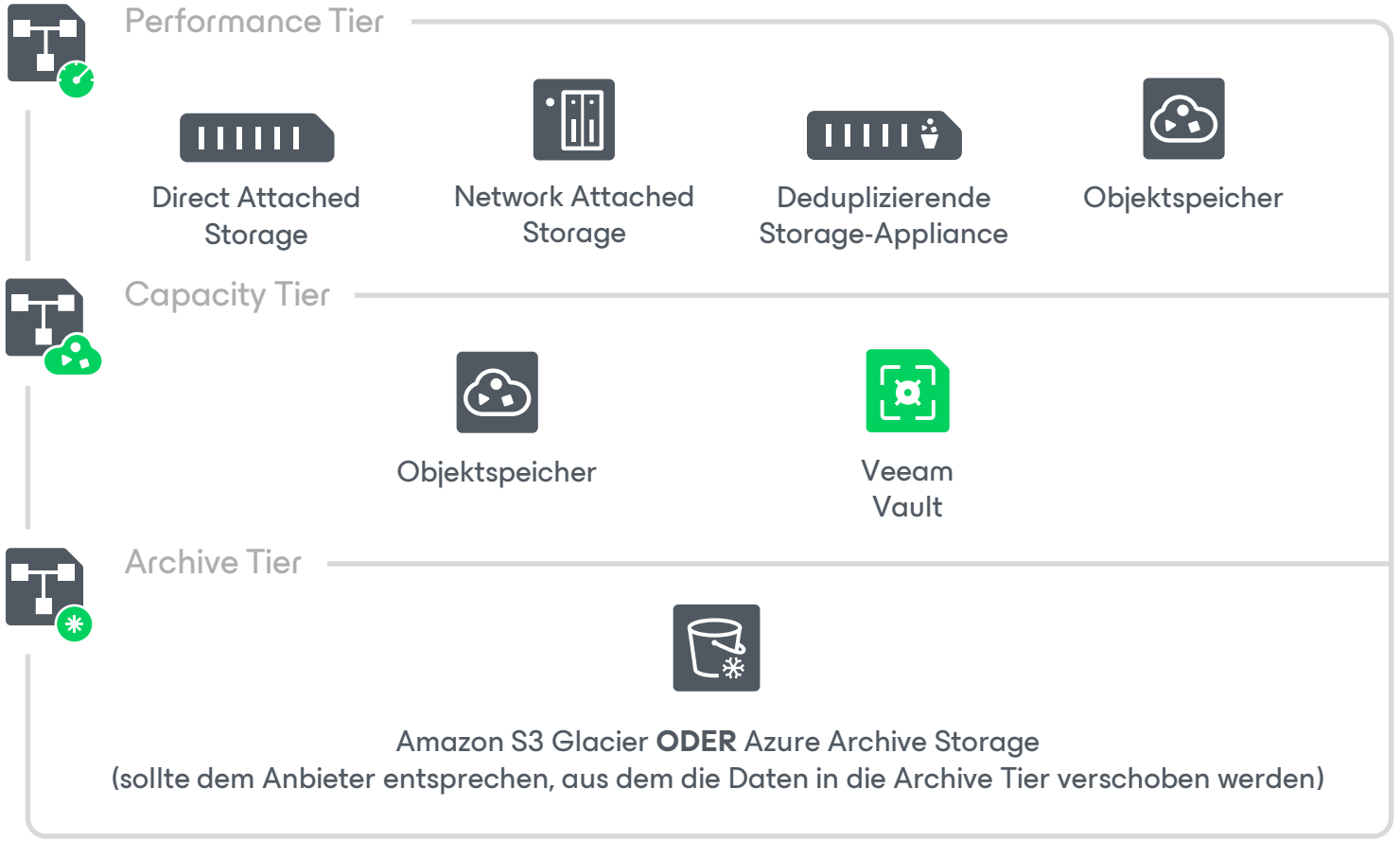
© 2025 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

Verhinderung der Verschlüsselung/Löschung von Backup-Daten

Scale–Out Backup Repository (SOBR)

Ein skalierbares Repository-System mit Unterstützung für Multi-Tier-Storage.

Es umfasst eine Performance Tier (lokaler oder gemeinsam genutzter Speicher) und kann um Capacity- und Archive-Tiers erweitert werden, was horizontale Skalierung für unterschiedliche Speicheranforderungen ermöglicht.



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Verhinderung der Verschlüsselung/Löschung von Backup-Daten

Unveränderlichkeit

Definition von Unveränderlichkeit:

- Unveränderlichkeit bezeichnet den Zustand von Daten, der verhindert, dass sie verändert oder gelöscht werden.

Vorteile der Unveränderlichkeit:

- Stellt Datenintegrität und Sicherheit Sicher.
- Bietet Schutz vor Ransomware und versehentlichem Löschen.

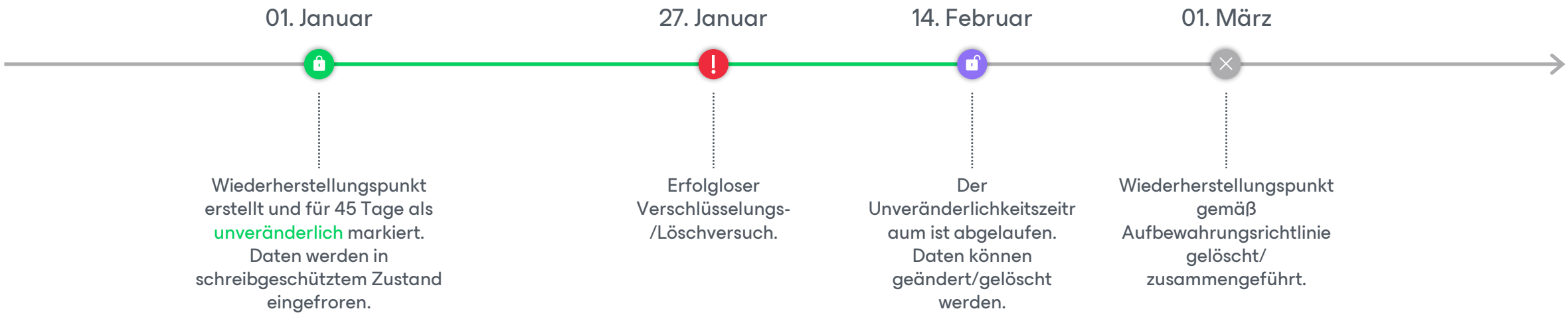
Unterstützte Arten unveränderlicher Repositories

- Veeam Hardened und Linux Immutable Repositories
- Veeam Vault
- Amazon, Azure, Google Cloud Storage und andere S3-kompatible Objektspeicher-Repositories
- HPE StoreOnce/Dell EMC Data Domain
- NFS/SMB
- Dell EMC Data Domain

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Verhinderung der Verschlüsselung/Löschung von Backup-Daten

Zeitachse der Unveränderlichkeit



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Verhinderung der Verschlüsselung/Löschung von Backup-Daten

Veeam Hardened Repository

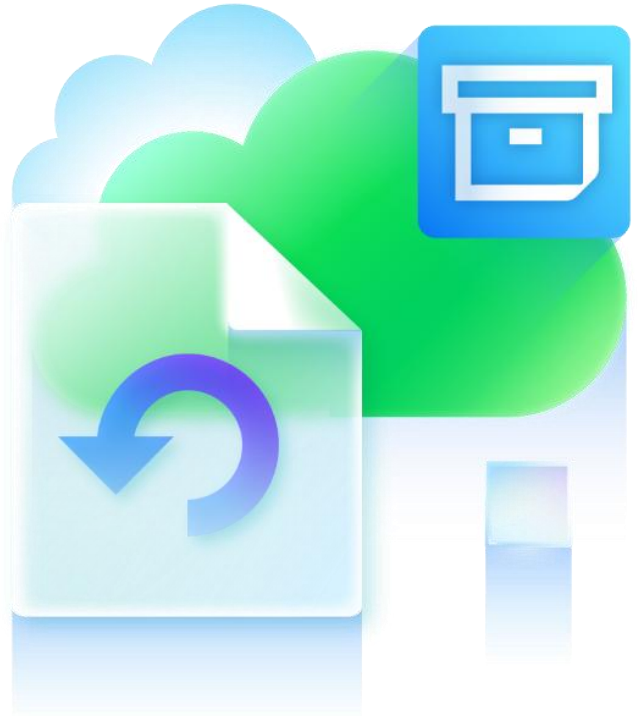
Ein Hardened Repository ist ein sicherer Speicher mit Unterstützung für Unveränderlichkeit, der dafür ausgelegt ist, Backup-Daten vor Löschung, Änderung oder Angriffen (wie Ransomware) zu schützen, selbst wenn jemand unautorisierten Zugriff erlangt.

- Kann auf generischem Linux betrieben werden, wodurch Vendor Lock-in vermieden wird und Organisationen ihre bevorzugte Hardware oder Linux-Distribution wählen können (z. B. Ubuntu, Debian, RHEL, SLES, Rocky usw.).

  Die Maschine muss die Systemanforderungen für Backup-Repositories erfüllen, und es gelten zusätzliche Anforderungen/Einschränkungen für das Hardened Repository.

- Kann über die Veeam Infrastructure Appliance installiert werden. JeOS, von Veeam verwaltet und aktualisiert, vereinfacht die Wartung durch automatisches Patching.

  Die Hardware muss auf der Red-Hat-Kompatibilitätsliste oder der Liste CIQ-zertifizierter Hardware stehen.

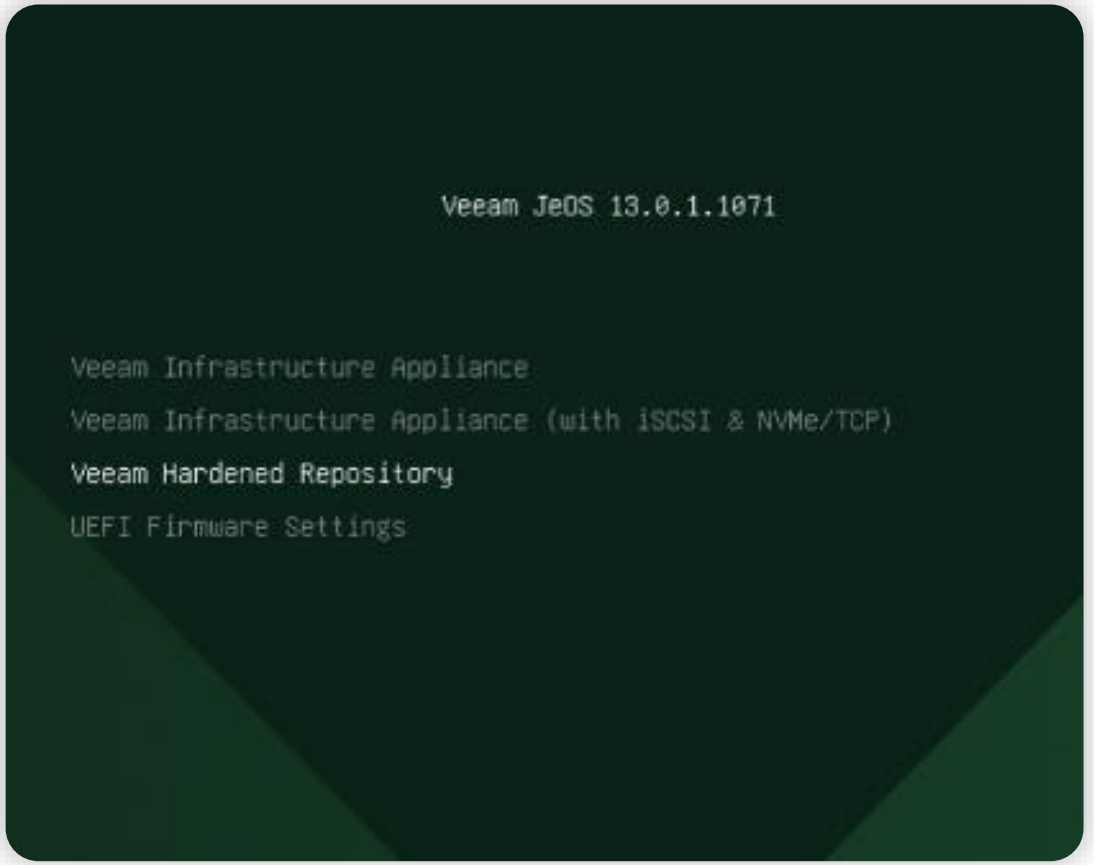


© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Verhinderung der Verschlüsselung/Löschung von Backup-Daten

Hardened Repository mit Veeam Infrastructure Appliance

- Angepasste Version eines minimalen Rocky Linux (JeOS)
- Einfache und schnelle Bereitstellung
- Vorgehärtet mit DISA-STIG-Sicherheitsprofil
- Vollständig automatisiertes Patchen von Schwachstellen



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Verhinderung der Verschlüsselung/Löschung von Backup-Daten

Funktionen des Hardened Repository

- Unveränderliche Backups: Dateien sind für einen benutzerdefinierten Zeitraum vor Änderung und Löschung geschützt, selbst wenn administrative Anmeldedaten kompromittiert werden. Dadurch wird sichergestellt, dass Backups nicht durch Malware, Ransomware oder versehentliche Administratoraktionen verändert oder gelöscht werden können.

- Air-Gap-ähnlicher Schutz: Das Repository wird gehärtet, indem der Zugriff eingeschränkt und Protokolle wie SSH deaktiviert werden, wodurch die Angriffsfläche minimiert wird und es als „undurchdringliche Black Box“ für Backup-Dateien fungiert.

- Schutz vor Insider-Bedrohungen: Durch die Verwendung von Einmal-Anmeldedaten und die Deaktivierung des Root-Zugriffs für Backup-Prozesse reduziert das Repository Risiken, selbst wenn der zentrale Veeam-Server kompromittiert wird.

- Speichereffizienz: In Kombination mit dem XFS-Dateisystem profitiert es von Block-Cloning-Technologie für effiziente synthetische Vollbackups, reduzierte Festplattennutzung und schnellere Backup-Vorgänge.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Risiko #3

Malware in Backups

Die Wiederherstellung aus einem infizierten Backup kann Malware erneut in die Produktionsumgebung einbringen, was zu erneuten Infektionszyklen und potenzieller Datenbeschädigung über Systeme hinweg führen kann.

Veeam-Sicherheit über den gesamten Backup-Lebenszyklus hinweg

Vorher

Während des Backups

Wiederherstellung

Veeam Threat Center

- Veeam Incident API
- Security & Compliance Analyzer
- Data Observability & Analytics
- Recon Scanner von Coveware

- Inline-Entropieanalyse
- Analyse der Dateisystemaktivität
- IoC Tools Scanner

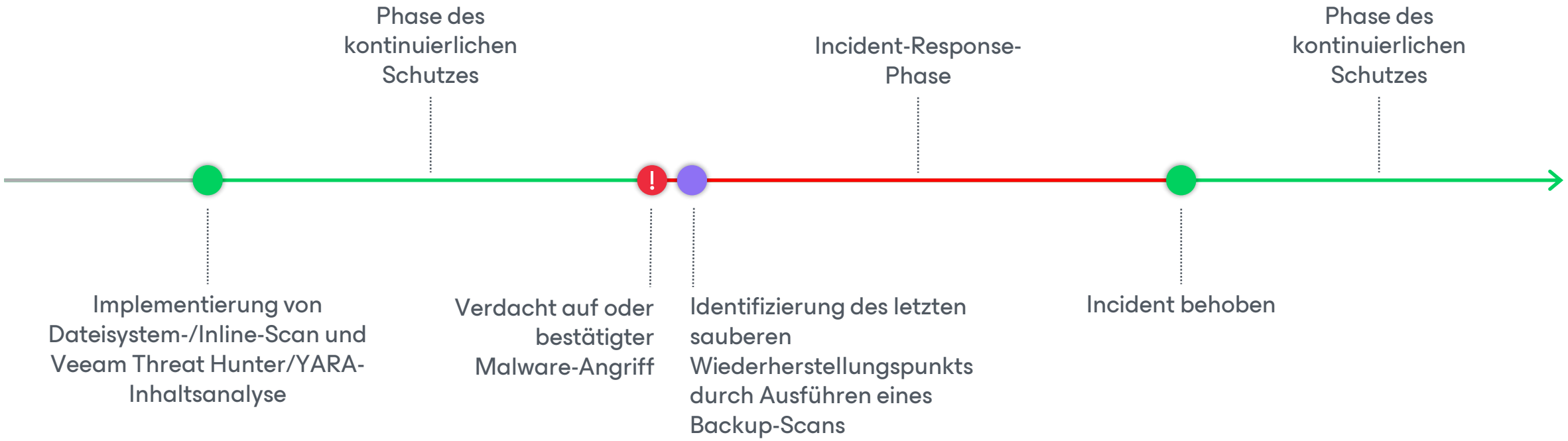
- Secure Restore
- YARA-regelbasiertes Scannen
- Threat Hunter
- Orchestrated Restore & Clean Room Recovery

Veeam Data Platform - Foundation
Veeam Data Platform - Advanced
Veeam Data Platform - Premium

Microsoft Sentinel | CROWDSTRIKE | splunk> | paloalto NETWORKS | CORTEX XSIAM

Malware in Backups

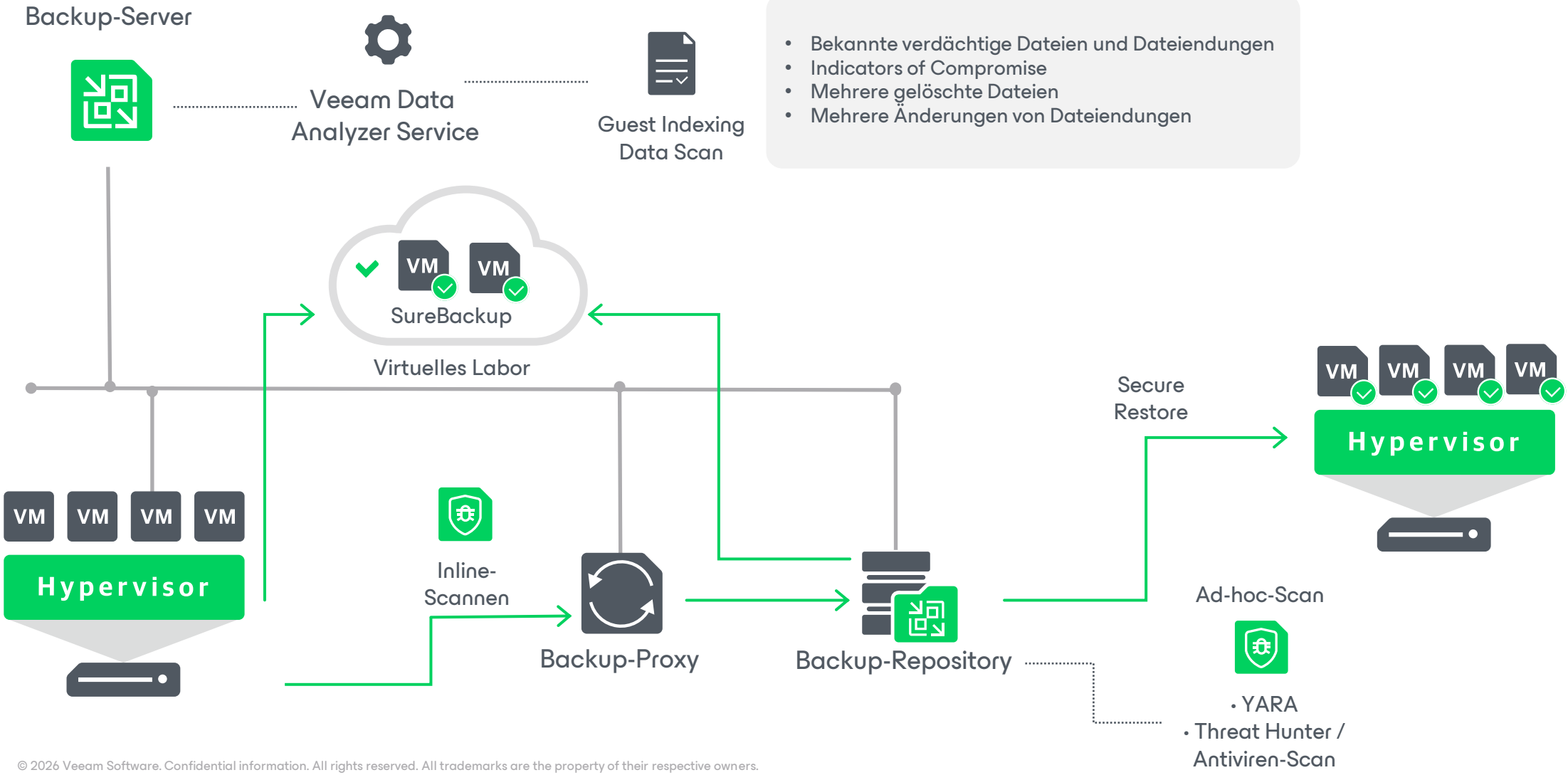
Vereinfachter Workflow



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Malware Detection

Malware-Erkennungsphasen während der Lebensdauer einer Backup-Datei



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Malware in Backups

Wie erkennt man Malware?

Analyse der Dateisystemaktivität – wird während des Backup-Jobs verwendet und scannt Guest-Indexierungsdaten auf: bekannte verdächtige Dateien und Dateiendungen, gelöschte Dateien, Änderungen von Dateiendungen.

Indicators of Compromise Tools Scanner – Indicators of Compromise sind Nicht-Malware-Programme. Ihre unerwartete Präsenz auf einem System kann jedoch auf ein Sicherheitsrisiko hinweisen.

Inline Scan (Entropieanalyse) – scannt während des Backup-Jobs Blöcke im Datenstrom auf: durch Malware verschlüsselte Dateien, von Malware erstellte Artefakte wie Onion-Links sowie von Medusa und Clop erstellte Hinweise.

Signaturbasierte Erkennung (Veeam Threat Hunter) – kann während Scan Backup, Secure Restore und SureBackup verwendet werden. Eine Alternative zu Drittanbieter-Antiviruslösungen, die in VBR integriert werden kann. Der Einsatz einer signaturbasierten Erkennungs-Engine, wie Antivirus, in der Produktionsumgebung und einer anderen Engine (Veeam Threat Hunter) mit einem anderen Satz von Malware-Definitionen für Backups ist eine bewährte Praxis. Markiert infizierte Objekte.

Regelbasierte Erkennung (YARA) – kann wie die signaturbasierte Erkennung während Scan Backup, Secure Restore und SureBackup verwendet werden. Ermöglicht die Erstellung benutzerdefinierter Regeln zur Identifizierung von Malware anhand textueller oder binärer Muster. Markiert infizierte Objekte.

Drittanbieterlösungen – es ist möglich, die Veeam Incident API zu verwenden, um eine Anfrage zu erkannter Malware-Aktivität an Veeam Backup & Replication zu senden und eine Maschine als infiziert zu markieren.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Malware in Backups

Warum wird Veeam Threat Hunter gegenüber Drittanbieter-AV empfohlen?

- Automatisch auf jedem Mount-Server installiert
- 3- bis 6-mal schneller als Windows Defender
- Verwendet Signaturen, die spezifischer auf Backups ausgelegt sind
- Vergleichbare AV-CPU- und RAM-Auslastung trotz höherem Durchsatz
- Proprietäre Engine ohne vom Benutzer anpassbare Signaturen
- In Veeam Data Platform Advanced enthalten: keine zusätzlichen AV-Lizenzgebühren

Der Wechsel zu einer Drittanbieter-AV-Lösung ist jederzeit eine Option, wenn Sie dies wünschen.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Malware in Backups

YARA-Regeln Leitfaden: Was sie sind und wie man sie erstellt

Was ist YARA und wie erstellt man YARA-Regeln?

```
rule RuleName {
    meta:
        author = "Security Team"
        description = "Custom threat detection"
        date = "2026-04-30"

    strings:
        $string_a = "unique_malware_string"
        $hex_b = { E2 34 A1 C8 23 FB }
        $regex_c = /malicious_pattern/

    condition:
        $string_a or ($hex_b and $regex_c)
}
```

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Malware in Backups

Wo findet man einsatzbereite YARA-Regeln?

Öffentliche Repositories

Es gibt zahlreiche Community-getriebene Repositories. Einige davon werden recht häufig aktualisiert. Einfach googeln oder die bevorzugte KI fragen.

Einige Überlegungen:

- Nicht alle öffentlichen Regeln erfüllen dieselben Qualitätsstandards. Organisationen sollten Regeln vor der Bereitstellung sowohl gegen schädliche Samples als auch gegen saubere Dateien validieren, um False Positives zu minimieren.
- Komplexe Regeln mit mehreren Bedingungen können die Scan-Performance erheblich verlangsamen. Zum Beispiel: Regeln sollten kurze Strings (weniger als 4 Byte) vermeiden, Wildcards in Hex-Strings minimieren und Regex sparsam mit festen 4-Byte-Ankern verwenden.

Generatoren und LLMs

Einige dieser Tools sind Open Source und von der Community erstellt, andere stammen von bekannten Sicherheitsunternehmen. Auch hier helfen Google/KI weiter.

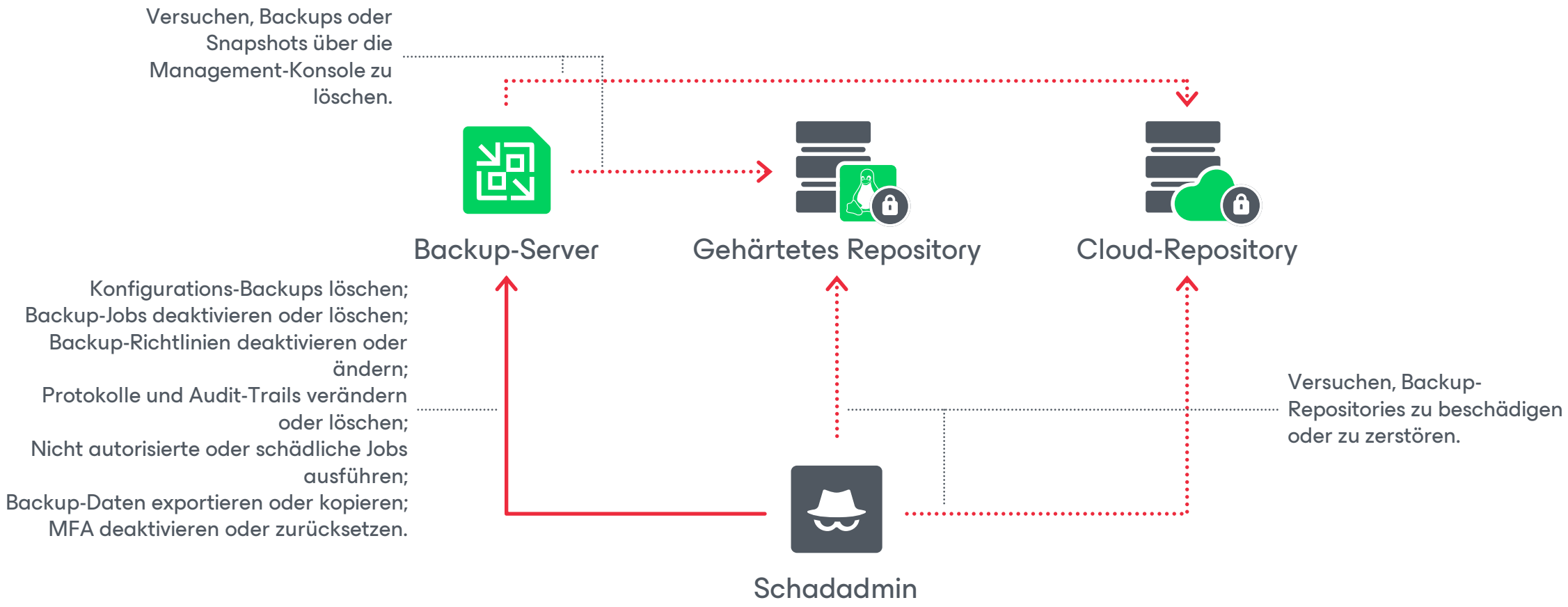
© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Risiko #4

Insider-Bedrohungen

Statistik: Authentifizierungsbasierte Angriffe und Insider-Bedrohungen nehmen zu, wobei privilegierte Benutzer erweiterten Zugriff auf kritische Backup-Infrastrukturen haben.

Insider-Bedrohungen



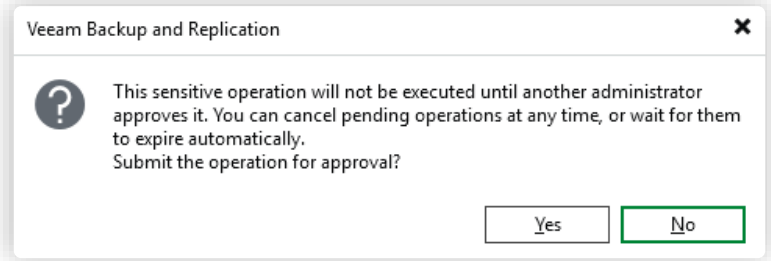
© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Insider-Bedrohungen

Vier-Augen-Autorisierung

Wenn aktiviert, ist die Vier-Augen-Autorisierung erforderlich für:

- Löschen von Backups, Snapshots oder der Konfigurationsdatenbank
- Ändern oder Entfernen von Backup-Repositories und Speicher
- Verwalten von Benutzern, Gruppen und MFA-Einstellungen
- Aktivieren oder Ändern automatischer Abmelderichtlinien
- Änderungen an Unveränderlichkeitseinstellungen



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Insider-Bedrohungen

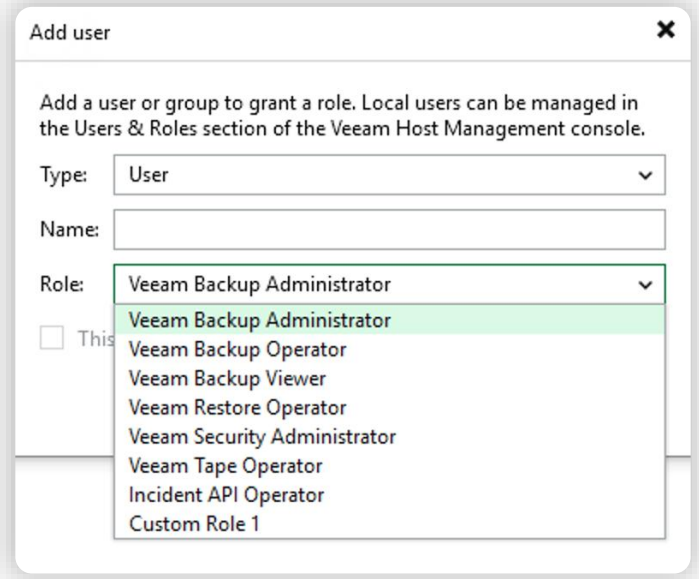
Verwenden Sie nur die minimal erforderlichen Berechtigungen

Verwenden Sie Rollen mit den minimal erforderlichen Berechtigungen, um die Aufgabe auszuführen.

Reduziert das Risiko unautorisierten Zugriffs und von Datenschutzverletzungen.

Minimiert die Angriffsfläche, indem Benutzerberechtigungen auf das Notwendige beschränkt werden.

Verbessert die allgemeine Systemsicherheit und Stabilität.



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

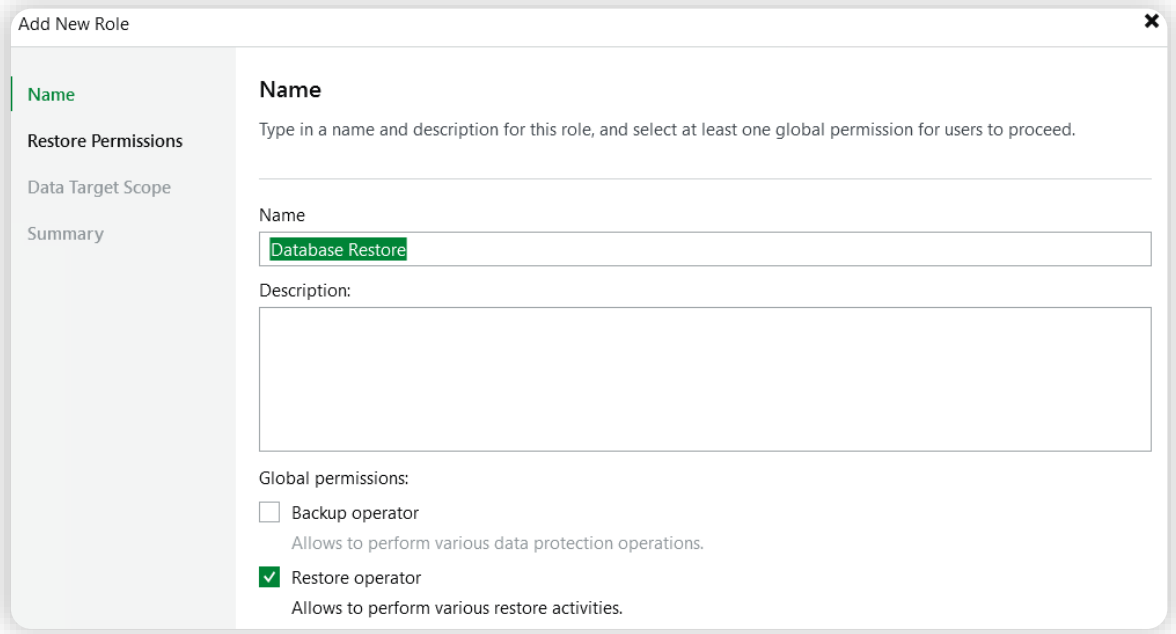
Insider-Bedrohungen

Erweiterte RBAC

Advanced RBAC ermöglicht es Ihnen, Benutzern ausschließlich Zugriff auf bestimmte Geltungsbereiche sowohl innerhalb der Backup-Infrastruktur als auch der Produktionsumgebung zu gewähren.

Erstellen Sie benutzerdefinierte Rollen, um den Zugriff zu steuern auf:

- Backup- und/oder Wiederherstellungsvorgänge
- Repositories
- Wiederherstellungsoptionen
- Infrastrukturobjekte



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Insider-Bedrohungen

Security Officer (Veeam Software Appliance)

Genehmigt Anfragen zur Zugriffserweiterung und andere sensible Vorgänge.
Der Security Officer kann die Anfrage jedoch nicht selbst initiieren.

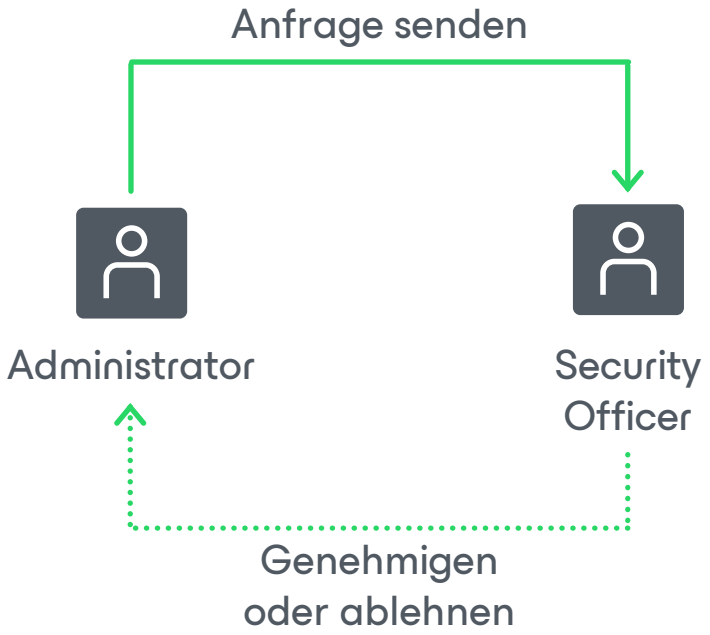
Root-Zugriff für Administratoren und Passwortzurücksetzung.

Wiederherstellung der Konfigurationssicherung.

Ermöglicht erweiterte Bereitstellungsoptionen:

- Hochverfügbarkeit
- Lockdown-Modus
- Agent-Bereitstellung zur Datenerfassung

Änderung der MFA-Einstellungen.



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Insider-Bedrohungen

Monitoring: Veeam ONE für Audits

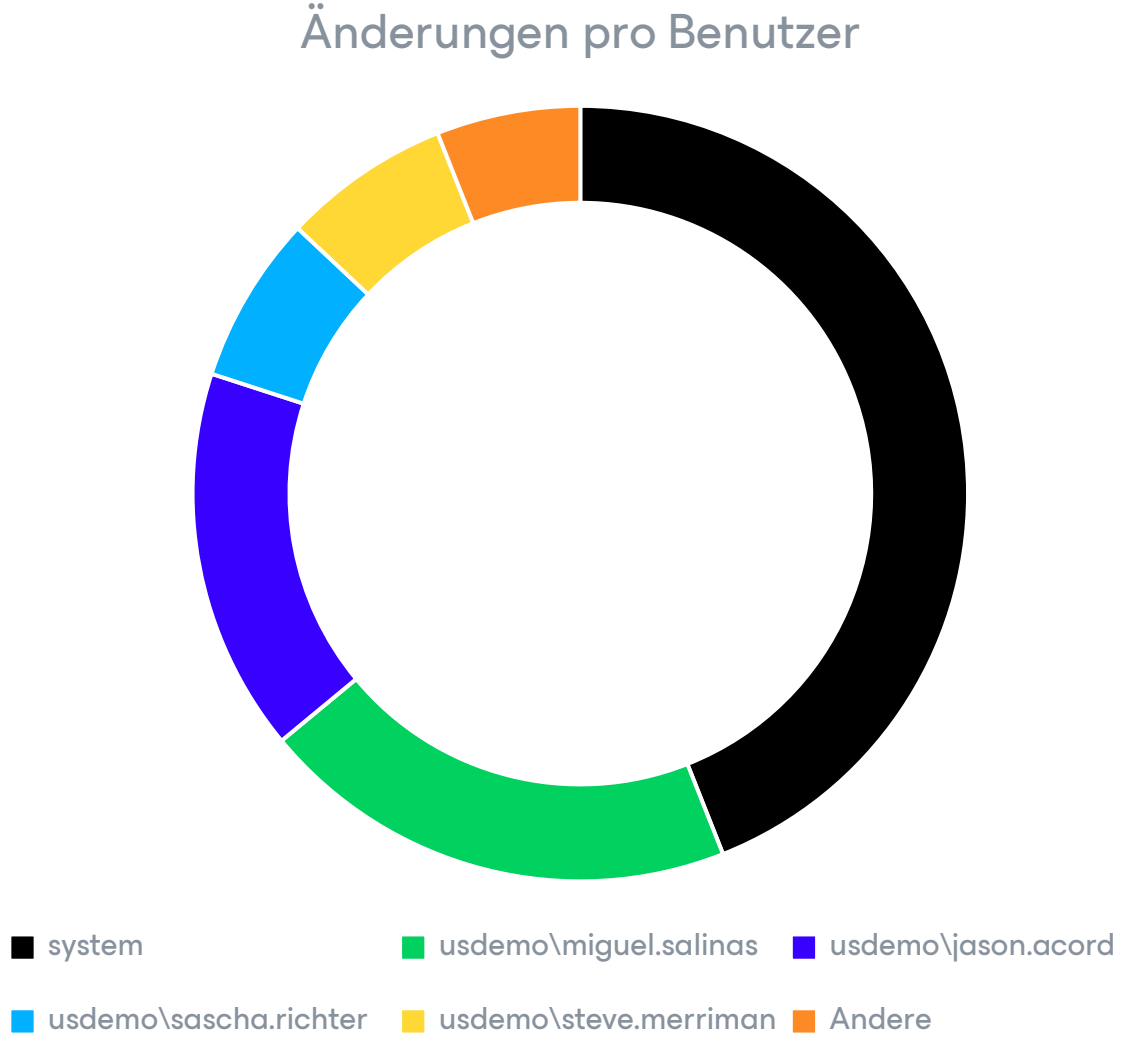
Audit-Informationen zu allen Arten von Wiederherstellungen für Nachvollziehbarkeit.

Detaillierte Protokolle von Änderungen an Job-Konfigurationen, einschließlich Zeitstempeln und Benutzerkonten.

Verfolgt Konfigurationsänderungen in virtuellen Umgebungen mit Details auf Benutzerebene.

Überwacht Änderungen an Zugriffen und Berechtigungen zur Einhaltung von Sicherheits-Compliance.

Erstellt umfassende Audit-Berichte für regulatorische und betriebliche Transparenz.



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Insider-Bedrohungen

Verfügen Sie über ein unveränderliches Backup?

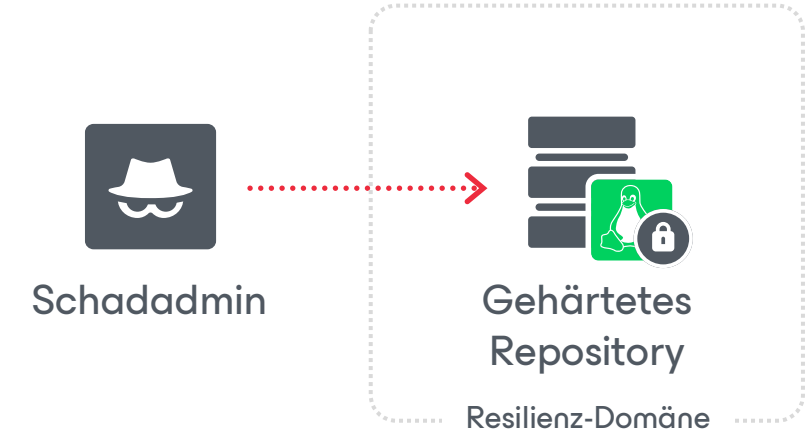
Einmalig verwendbare Linux-Anmeldedaten, nicht in der Veeam-Datenbank gespeichert

Veeam-Dienste steuern die Ports für den Datenverkehr (virtueller Air Gap)

SSH ist deaktiviert und für Veeam-Upgrades nicht erforderlich

Verhindert unautorisierte Änderung oder Löschung von Backups

Begrenzt Insider-Bedrohungen, indem die Möglichkeit eingeschränkt wird, gespeicherte Daten zu ändern oder zu löschen



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Risiko #5

Netzwerkbasierte laterale Bewegung

Statistik: Die mediane Verweildauer beträgt 26 Tage bei externer Benachrichtigung, aber nur 5 Tage in Ransomware-Fällen, in denen Angreifer die Opfer benachrichtigen.

Netzwerkbasierte laterale Bewegung

Was bedeutet das? Und wie hängt das mit Veeam zusammen?

Angreifer bleiben selten bei dem System stehen, das sie zuerst kompromittiert haben. Stattdessen kartieren sie die Umgebung, nehmen zusätzliche Systeme ins Visier und passen ihre Taktiken je nach vorgefundenen Sicherheitskontrollen an.

Laterale Bewegung kann legitime Tools nutzen (PowerShell- und BASH-Skripte, WMI, RDP, SSH, Nmap, SCP, Netzwerkfreigaben usw.), um sich in normale Aktivitäten einzufügen, wodurch sie besonders schwer zu erkennen ist.

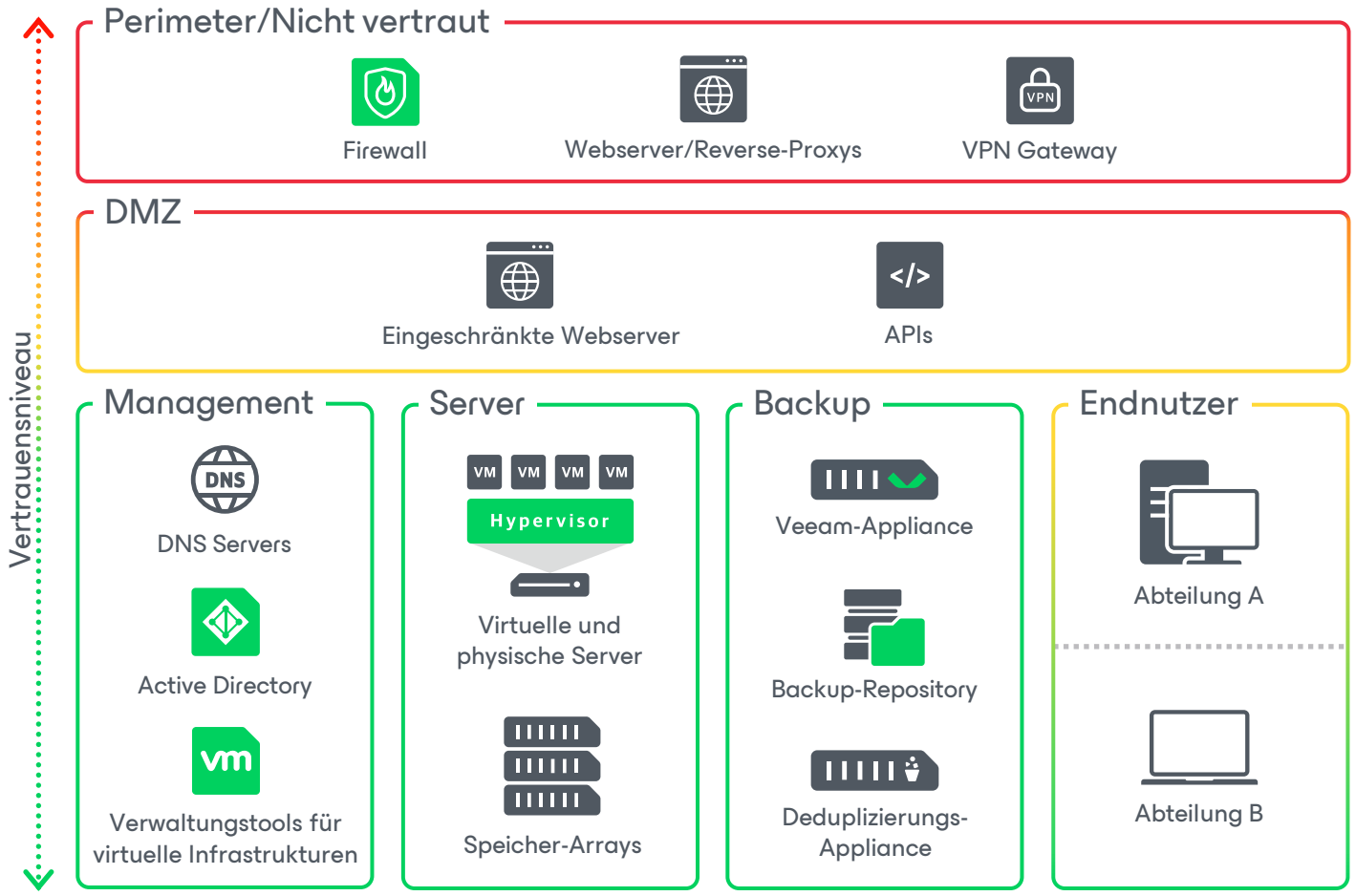
Angreifer nutzen Schwächen in der Netzwerksicherheit aus (z. B. unzureichende Segmentierung, weitreichende Berechtigungen, domänengebundene Backup-Server), um sich lateral zu bewegen und zusätzliche Systeme zu kompromittieren.

Wie Sie bereits wissen, ist die Backup-Infrastruktur ein hochwertiges Ziel für laterale Bewegung, da Angreifer die Disaster-Recovery-Fähigkeiten sabotieren wollen.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Netzwerkbasierte laterale Bewegung

Netzwerksegmentierung: Beispiel für Zonen



Begrenzt laterale Bewegung

Nur notwendige Kommunikation ist erlaubt. Angreifer können nicht einfach von kompromittierten zu kritischen Systemen springen.

Perfekte Synergie

Kombinieren Sie dies mit aktiver Bedrohungserkennung wie XDR/EDR, Honeypots zur Anlockung von Angreifern und SIEM für bessere Transparenz.

Compliance-Enabler

Segmentierte Architekturen unterstützen gesetzliche und regulatorische Verpflichtungen – und schützen die Organisation sowohl operativ als auch rechtlich.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

veeam

Netzwerkbasierte laterale Bewegung

Was gibt es außer Netzwerksegmentierung noch?

VBR-Sicherheits-Best-Practices: Härtung

Leitfaden zu SIEM (Security Information & Event Management)

Verschlüsselte Kommunikation

Veeam verschlüsselt Management-Verbindungen standardmäßig mit selbstsignierten TLS-Zertifikaten. Es ist jedoch möglich, ein von einer internen Zertifizierungsstelle signiertes Zertifikat zu verwenden, um bessere Kontrollmöglichkeiten zu erhalten.

Härtung der Backup-Infrastruktur

MFA, Key Management System, Vier-Augen-Prinzip, RBAC, keine Aufnahme in die AD-Domäne usw.

Monitoring

Veeam B&R/ONE erzeugt Echtzeitwarnungen bei Problemen wie Backup-Fehlern, Job-Anomalien oder ungewöhnlichen Aktivitätsspitzen, die auf Ransomware oder eine Kompromittierung der Infrastruktur hinweisen können, und leitet diese Warnungen direkt an SIEM weiter. SIEM kann diese mit Sicherheitstrends/Anomalien an anderer Stelle in Ihrem Netzwerk abgleichen und schnell aufzeigen, wenn Ihre Backup-Umgebung gefährdet ist.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Netzwerkbasierte laterale Bewegung

Hören Sie nicht auf, Shadow-IT zu bekämpfen!

Erweitert die Angriffsflächen

Nicht autorisierte Apps, Cloud-Plattformen oder Remote-Access-Tools schaffen versteckte Pfade, die Angreifer ausnutzen können. Diese Pfade umgehen häufig standardmäßige Netzwerkkontrollen und Monitoring.

Offenlegung von Anmeldedaten und Bridging

Benutzer speichern oder teilen Passwörter möglicherweise über nicht freigegebene Kanäle wie E-Mail, Chat-Apps oder persönliche Dateispeicher, wodurch Angreifer Einstiegspunkte für anmeldeinformationsbasierte laterale Bewegung über Segmente hinweg erhalten.

Erleichtert verdeckte laterale Bewegung

Angreifer können Shadow-IT-Tools nutzen, um Daten zwischenzulagern, Befehle weiterzuleiten oder Malware zu übertragen – und sich dabei in regulären Datenverkehr einzufügen, wodurch die Erkennung mit herkömmlichen Mitteln deutlich erschwert wird.

Reduziert Monitoring und verwertbare Erkenntnisse

Für traditionelle SIEMs und Backup-Monitoring ist es schwieriger, laterale Bewegung zu erkennen, die Shadow IT nutzt, da Protokolle und Datenverkehr möglicherweise nicht über freigegebene oder überwachte Kanäle laufen.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Risiko #6

Datenvergiftung

Dieses Risiko nimmt zu, da immer mehr Organisationen KI-/ML-Pipelines produktiv einsetzen, die mit gesicherten Daten trainieren – eine unbemerkte Verfälschung des Trainingsdatensatzes verfälscht jedes daraus trainierte Modell.

Datenvergiftung

Was ist Datenvergiftung?

Datenvergiftung in Backups bezeichnet einen ausgefeilten Cyberangriff, bei dem Angreifer die ursprünglichen Daten subtil verändern oder beschädigen, bevor sie gesichert werden. Diese bösartigen Änderungen bleiben oft über lange Zeit unbemerkt und machen Sicherungskopien unzuverlässig oder kompromittiert, wodurch die gesamte Wiederherstellungsstrategie untergraben wird.

Die Änderungen werden so vorgenommen, dass sie wie normale Fehler oder routinemäßige Aktualisierungen aussehen. Über Wochen, Monate oder sogar Jahre summieren sich diese kleinen Änderungen. Irgendwann sind die Daten so stark verfälscht, dass sie Probleme verursachen – etwa finanzielle Verluste, falsche Statistiken oder Fehler in Berichten und Entscheidungen.

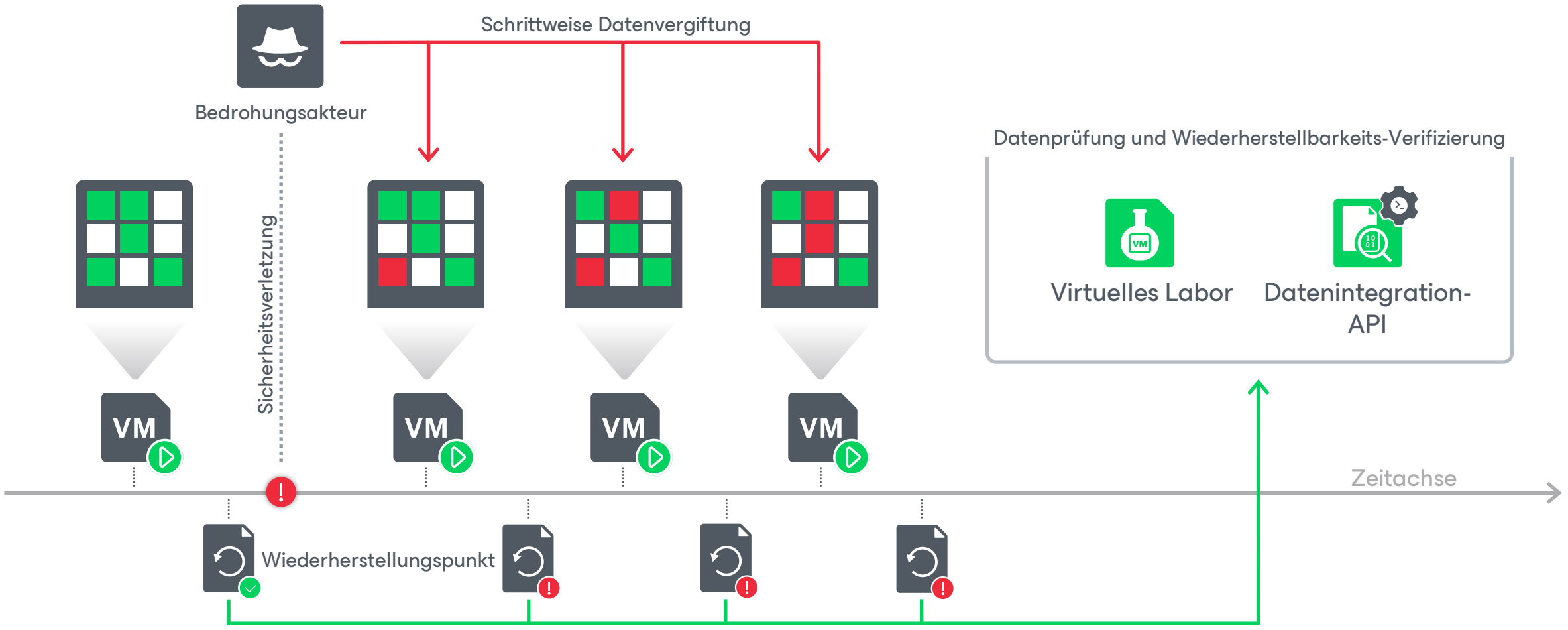
Im Gegensatz zu klassischer Ransomware oder destruktiven Angriffen zielt Datenvergiftung auf die Validität und Integrität der Daten selbst ab und stellt sicher, dass selbst wiederhergestellte Dateien beschädigt sind oder ungültige/veränderte Daten enthalten.

Solche Angriffe bleiben oft unbemerkt, bis Daten validiert werden oder eine Wiederherstellung versucht wird, was kostspielige Ausfallzeiten und Datenverluste verursachen kann.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Datenvergiftung

Schrittweise oder „Low and Slow“



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Datenvergiftung

Clean-Room-Datenwiederherstellung: Verbesserung von Sicherheit und Datenintegrität

Virtual Lab und Disk Publishing (Data Integration API)

Das Virtual Lab ist eine „Sandbox"-Umgebung, mit der SureBackup-Jobs Ihre Backups testen können, ohne Produktionssysteme zu beeinträchtigen. Diese Umgebung ermöglicht es Ihnen, Backups wiederholt sowohl auf Wiederherstellbarkeit als auch auf inhaltliche Integrität zu prüfen.

SureBackup überprüft, ob kritische Dienste – wie Datenbanken, Active Directory und E-Mail-Systeme – innerhalb der Sandbox ordnungsgemäß funktionieren. Ungewöhnliches Anwendungsverhalten während dieser Tests kann auf verdeckte Formen der Datenvergiftung hinweisen.

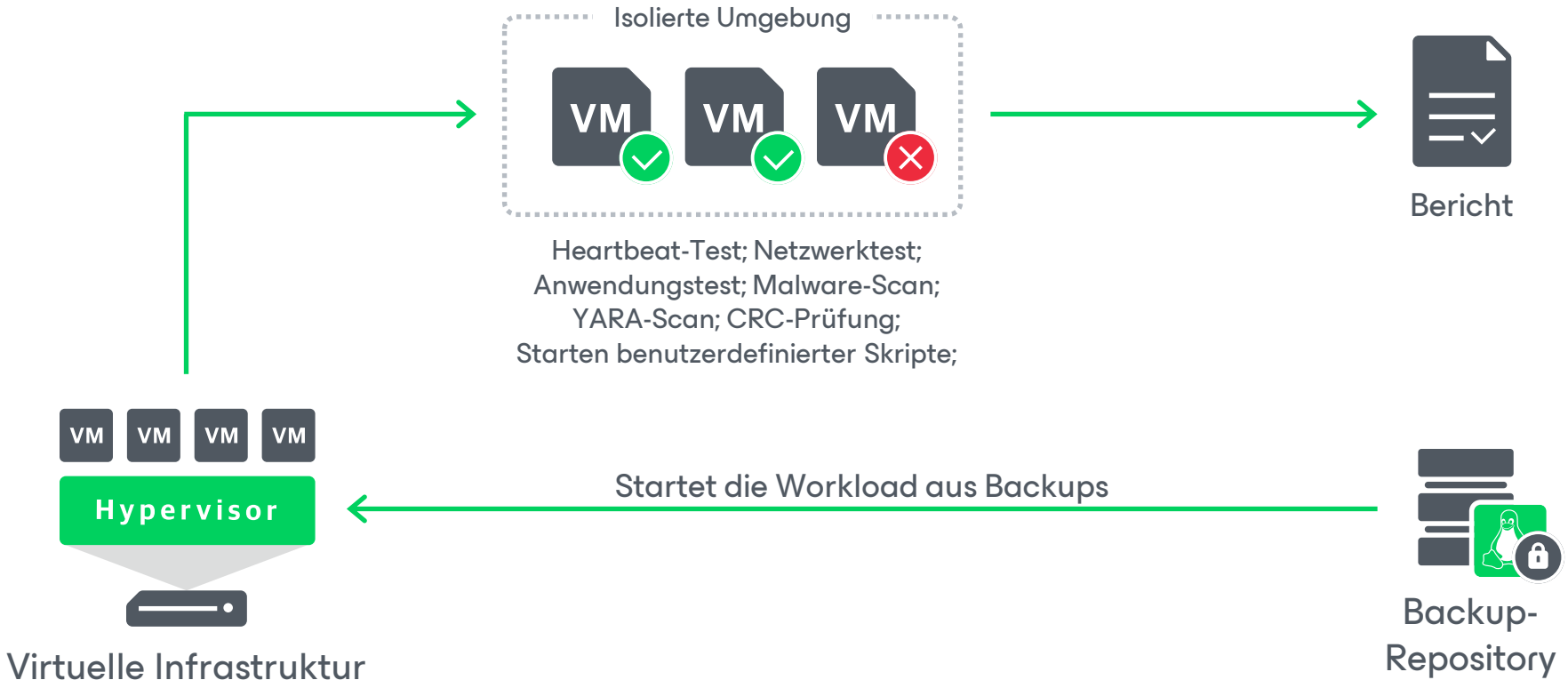
Disk Publishing (Data Integration API) ermöglicht das Mounten von Backup-Daten ohne vollständige Wiederherstellung, sodass Sie benutzerdefinierte Skripte, Data Mining, Klassifizierung, Analysen oder Forensik-Tools im Rahmen automatisierter Workflows auf Backup-Daten anwenden können.

Sie können aktuelle Backups mit vertrauenswürdigen sauberen Backups vergleichen, um Data Drift oder unautorisierte Änderungen zu erkennen. Verdächtige oder veränderte Datensätze können für eine detaillierte menschliche Analyse oder umfassende Berichterstellung exportiert werden.

Sie können den Prozess außerdem programmatisch über von Veeam bereitgestellte RESTful-Endpunkte steuern.

Datenvergiftung

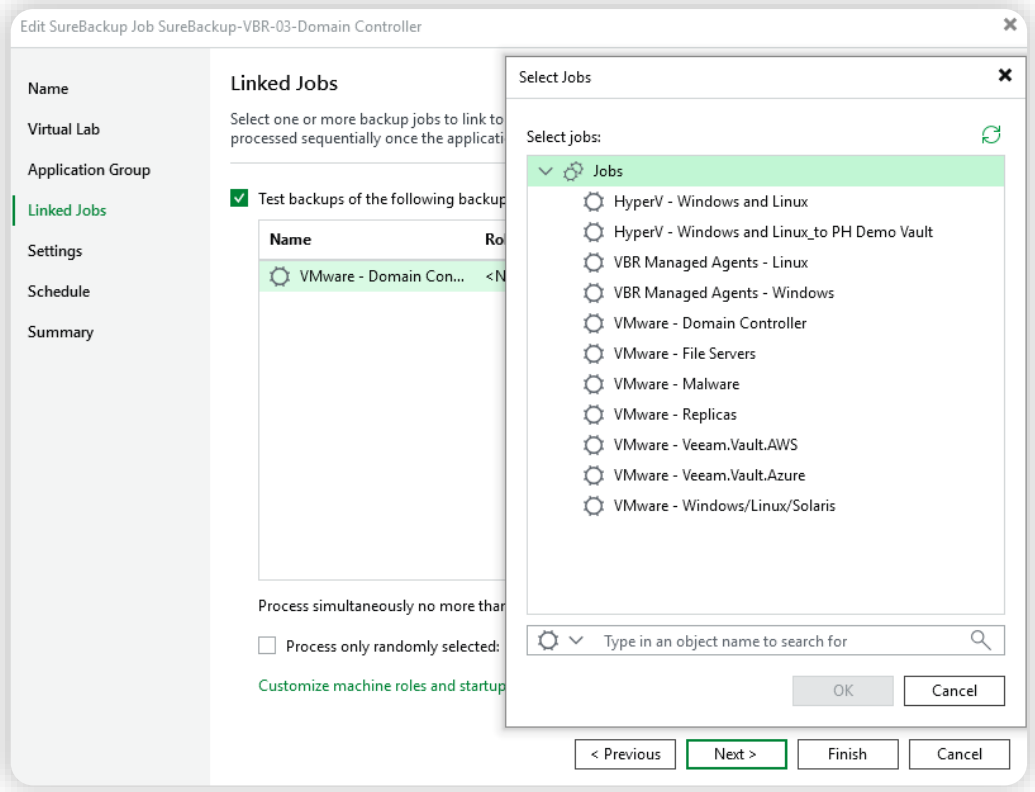
SureBackup-Workflow

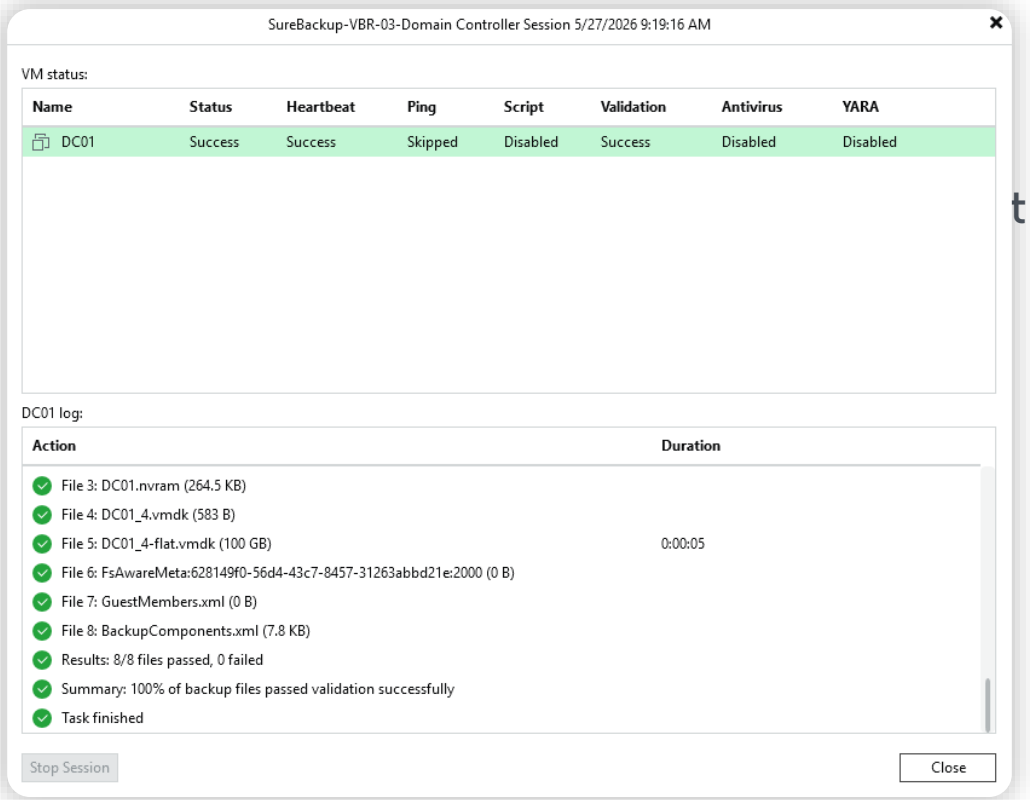


© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Datenvergiftung

SureBackup

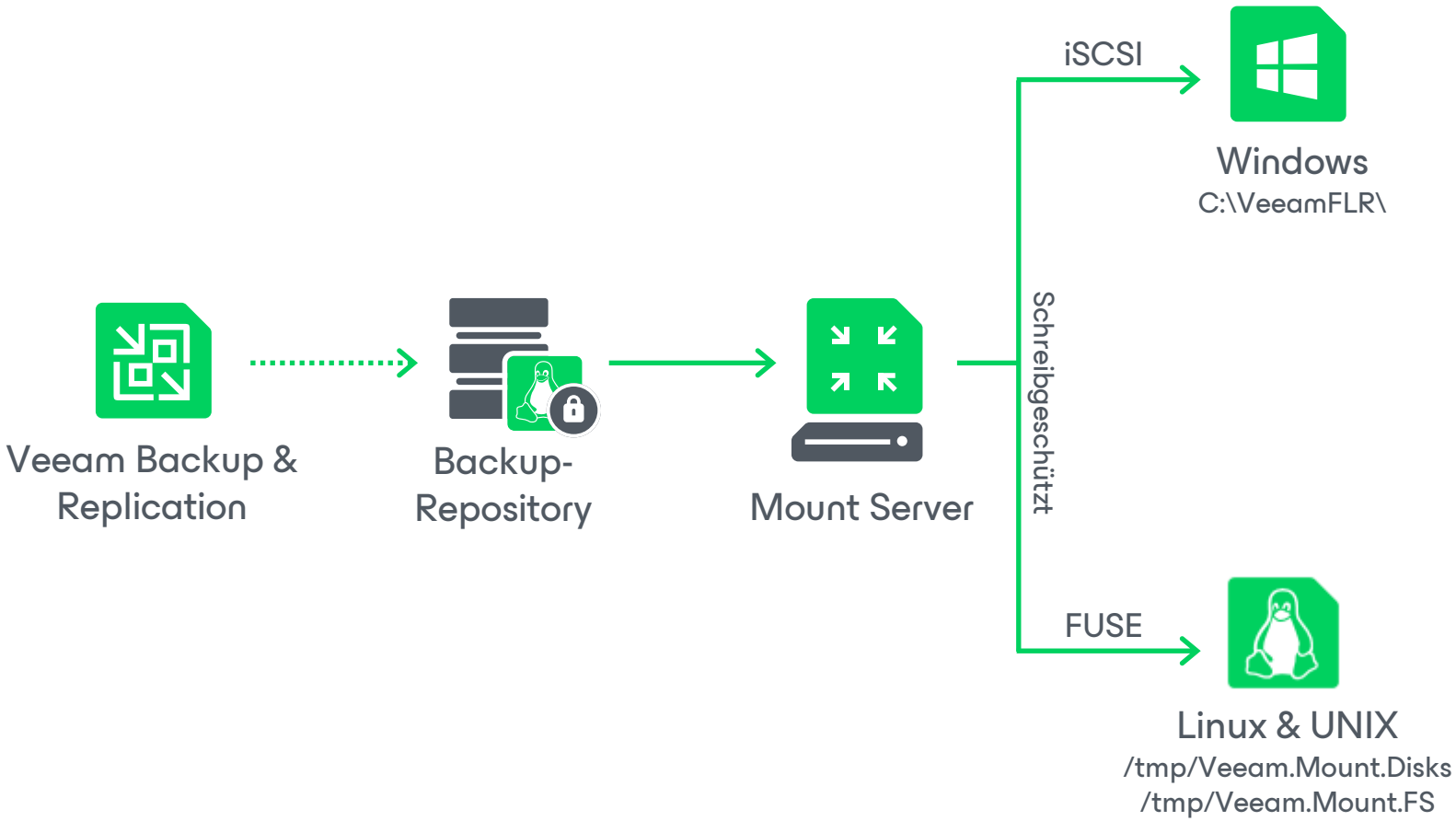




© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Datenvergiftung

Disk-Publishing-Workflow



Anwendungsfälle

- Data Mining
- Klassifizierung
- Analysen
- Forensik-Tools
- Sicherheitsanalyse
- Malware-Scanning
- eDiscovery
- DSGVO-Auditing
- ML-Anwendungen
- Datenvergleich
- Integritätsprüfung

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Datenvergiftung

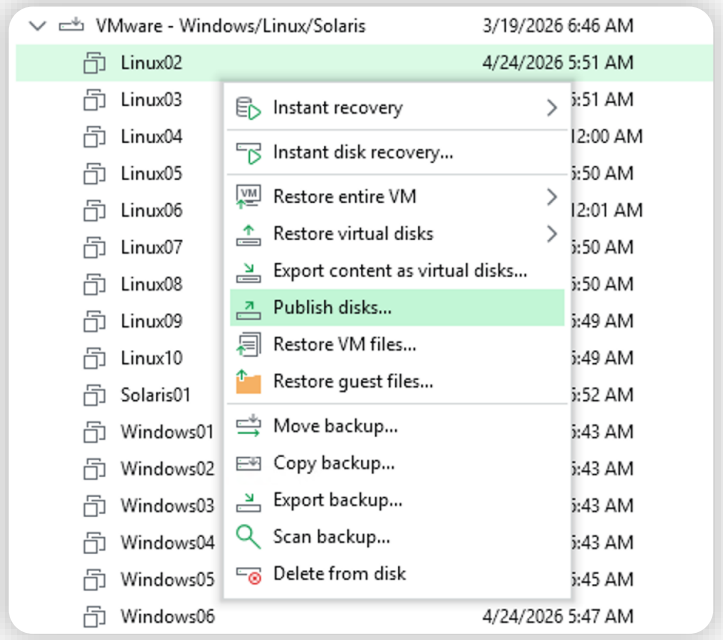
Disk Publishing (Data Integration API)

Die Data Integration API (REST) ist die programmatische Version von „Publish disks…“.

Sie ermöglicht Automatisierung, Integration und wiederholbare Workflows.

Im Grunde genommen ist es das „Backend“, das die „Publish-Disks…“ hinter den Kulissen nutzen.

Es ist auch möglich, PowerShell-Skripte zu verwenden, um „Publish disks…“ zu automatisieren.



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Risiko #7

Allgemeine Schwachstellen der Umgebung

Vielen Organisationen fehlt es an geeigneten Sicherheitskonfigurationen, obwohl Playbooks und Best Practices vorhanden sind.

Eine Kette ist nur so stark wie ihr schwächstes Glied...

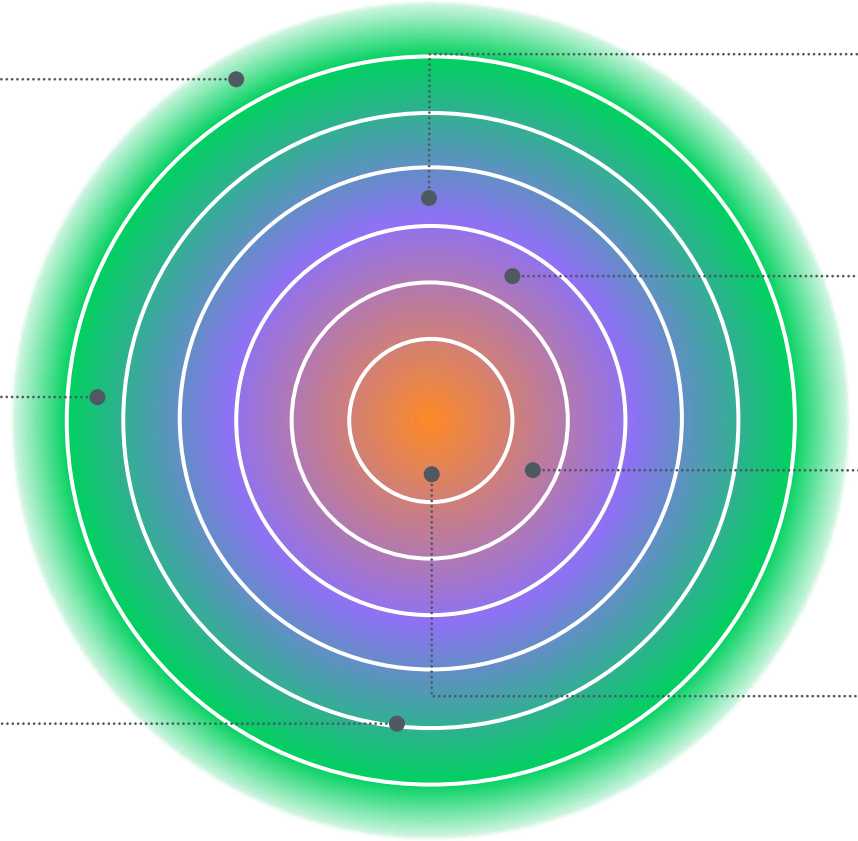
Allgemeine Schwachstellen der Umgebung

Sicherheitsebenen

Menschliche Ebene
Die meisten Sicherheitsverletzungen nutzen menschliche Fehler aus – Phishing, Social Engineering, schwache Passwörter.

Perimeter-Sicherheitsebene
Dies ist der „äußere Zaun“ – hier schrecken Sie externe Angreifer ab oder blockieren sie.

Netzwerksicherheitsebene
Verhindert laterale Bewegung und begrenzt die Ausbreitung von Bedrohungen innerhalb Ihrer Umgebung.



Endpoint-Sicherheitsebene
Jedes Gerät (PC, Server, Mobilgerät) ist ein potenzieller Einstiegspunkt

Anwendungssicherheitseben
Anwendungen sind häufige Ziele für Angriffe.

Datensicherheitsebene
Das eigentliche Ziel sind Ihre Daten – ob durch Diebstahl, Erpressung oder Sabotage.

Ebene geschäftskritischer Assets
Systeme/Daten, die für die Geschäftskontinuität essenziell sind, erfordern besondere Schutzmaßnahmen.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Allgemeine Schwachstellen der Umgebung

Es geht nicht nur um die VDP-Konfiguration

Stellen Sie sich vor, Sie konfigurieren einen neuen Server...

1. Würden Sie die Standardzugangsdaten ändern?
2. Würden Sie das Logging zu einem externen Monitoring-System konfigurieren?
3. Würden Sie die gesamte Firmware aktualisieren – und das regelmäßig?
4. Würden Sie sicherstellen, dass die Management-Schnittstellen in das isolierte *Management*-Netzsegment eingebunden werden?
5. Würden Sie ungenutzte physische Ports und Schnittstellen deaktivieren?
6. Würden Sie veraltete Management-/Authentifizierungsprotokolle (Telnet/NTLM/SNMPv1/HTTP) deaktivieren und nur die sichersten aktiv lassen (SSH/HTTPS)?
7. Würden Sie beim weiteren Konfigurieren den Hardening-Baseline-Vorgaben (DISA STIG, NIS2 usw.) folgen?

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Allgemeine Schwachstellen der Umgebung

Es geht nicht nur um die VDP-Konfiguration

Denken Sie allgemein über Ihre Umgebung nach...

1. Wann haben Sie zuletzt die Liste der Administratoren auf inaktive/„Geist“-Konten überprüft?
2. Wie viele aktive Firewall-Regeln erlauben mehr als nötig? Suchen Sie einfach nach „allow any“.
3. Haben Sie schon einmal einen Portscanner aus nicht vertrauenswürdigen bzw. halb vertrauenswürdigen Netzwerken ausgeführt?
4. Nutzen Sie Betriebssysteme, die sich bereits im End-of-Life-Status befinden?
5. Wie lange ist es her, dass Sie ein Sicherheitsereignis simuliert haben (ungültige Anmeldung, Rechteausweitung), um zu prüfen, ob es vom SIEM erfasst wurde?
6. Haben Sie ein Sicherheitstraining für Ihre Mitarbeitenden durchgeführt? Einschließlich simuliertem Phishing/Social Engineering, um reales Nutzerverhalten zu testen?
7. WLAN, physische Sicherheit, Endpoint-Hardening, Cloud(s)...

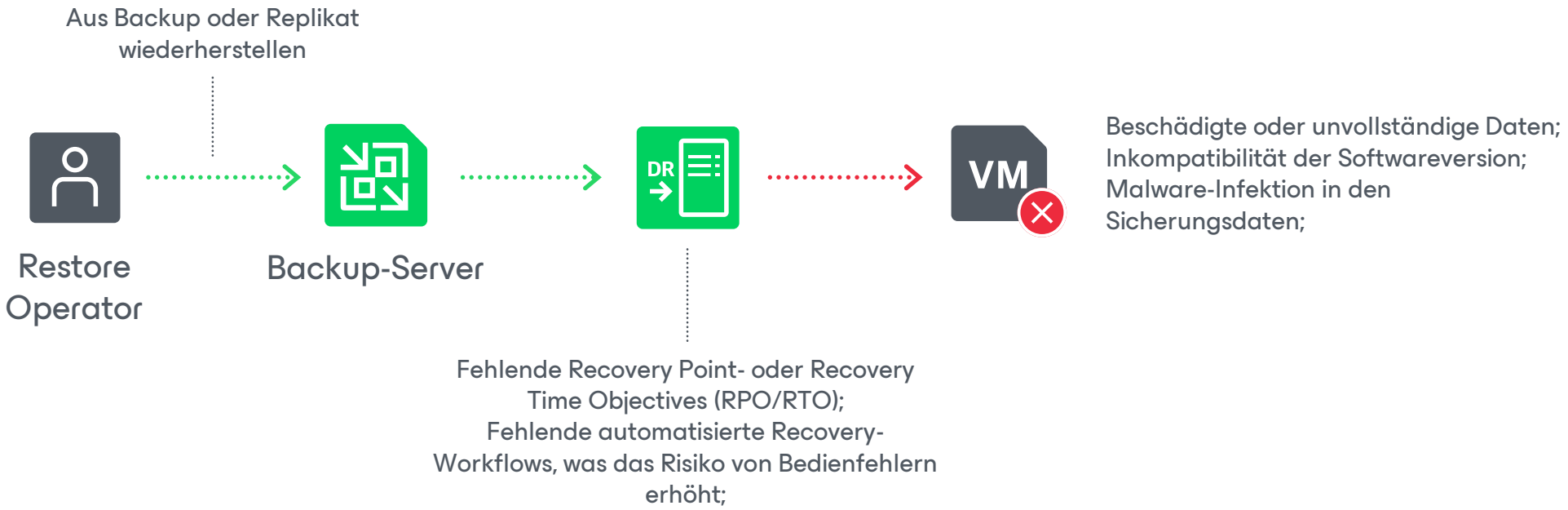
© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Risiko #8

Wiederherstellungs- und Orchestrierungsfehler

Fehler bei der Disaster Recovery und der Recovery-Orchestrierung werden häufig durch unzureichende Tests, veraltete Wiederherstellungspläne sowie fehlende Dokumentation oder Automatisierung verursacht.

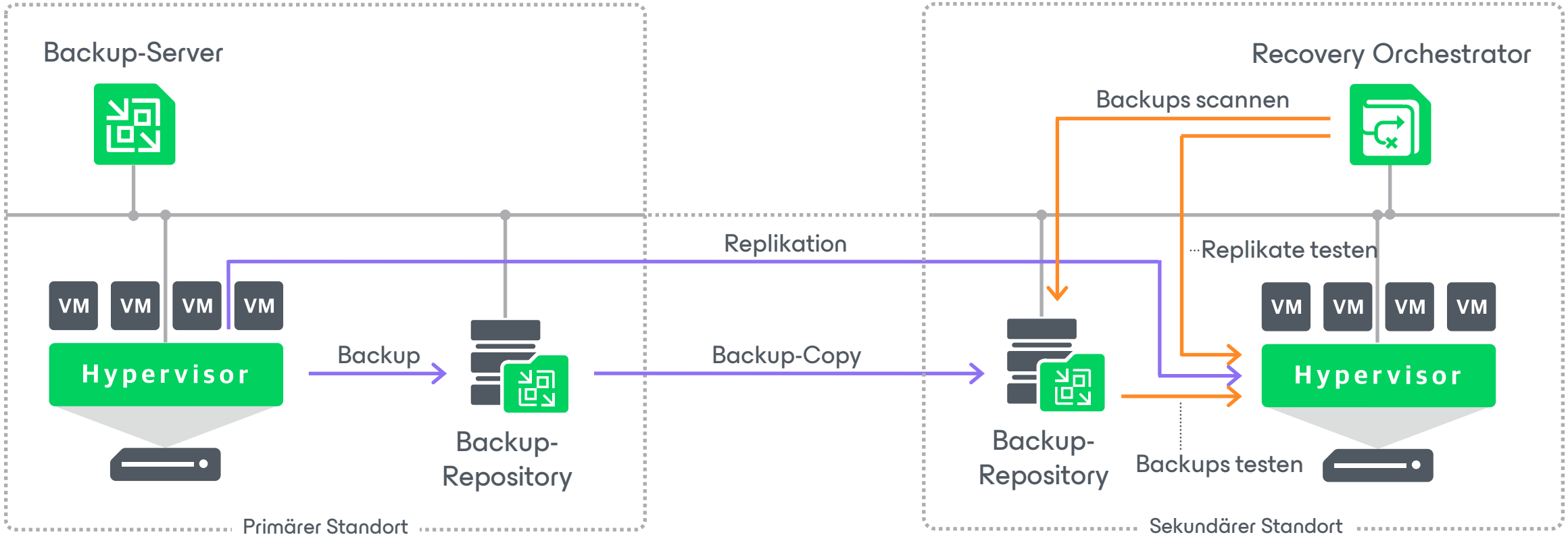
Wiederherstellungs- und Orchestrierungsfehler



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Wiederherstellungs- und Orchestrierungsfehler

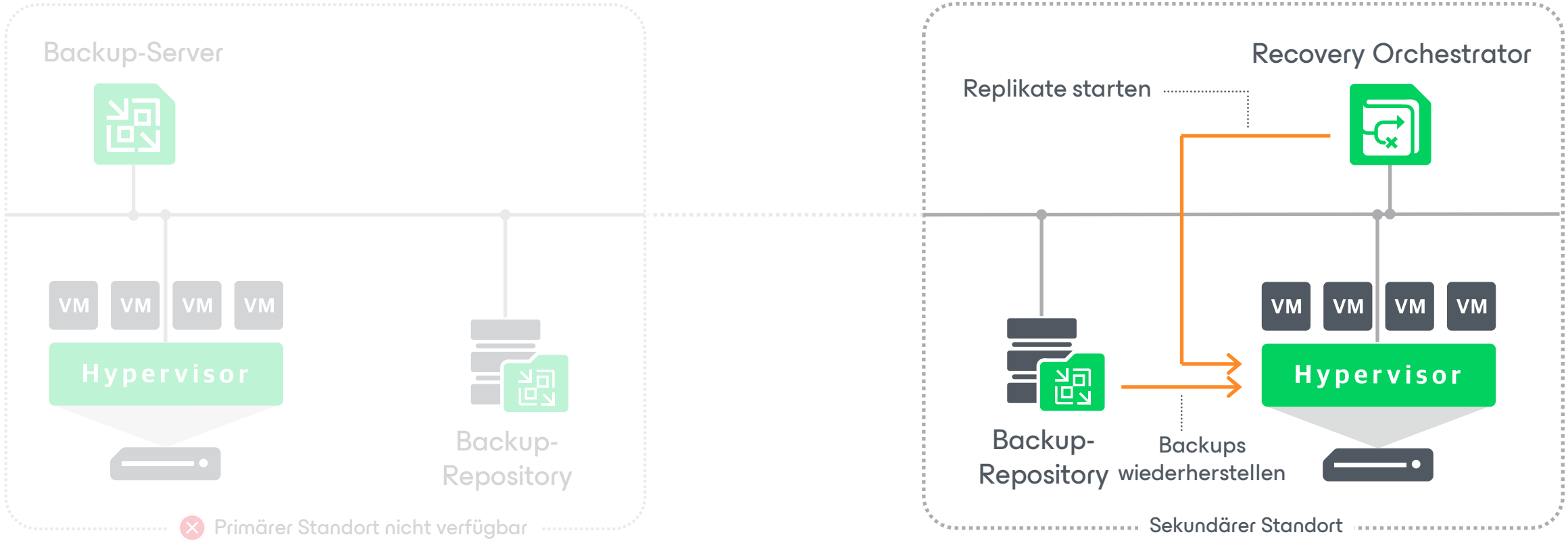
Regulärer Betrieb



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Wiederherstellungs- und Orchestrierungsfehler

Failover



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

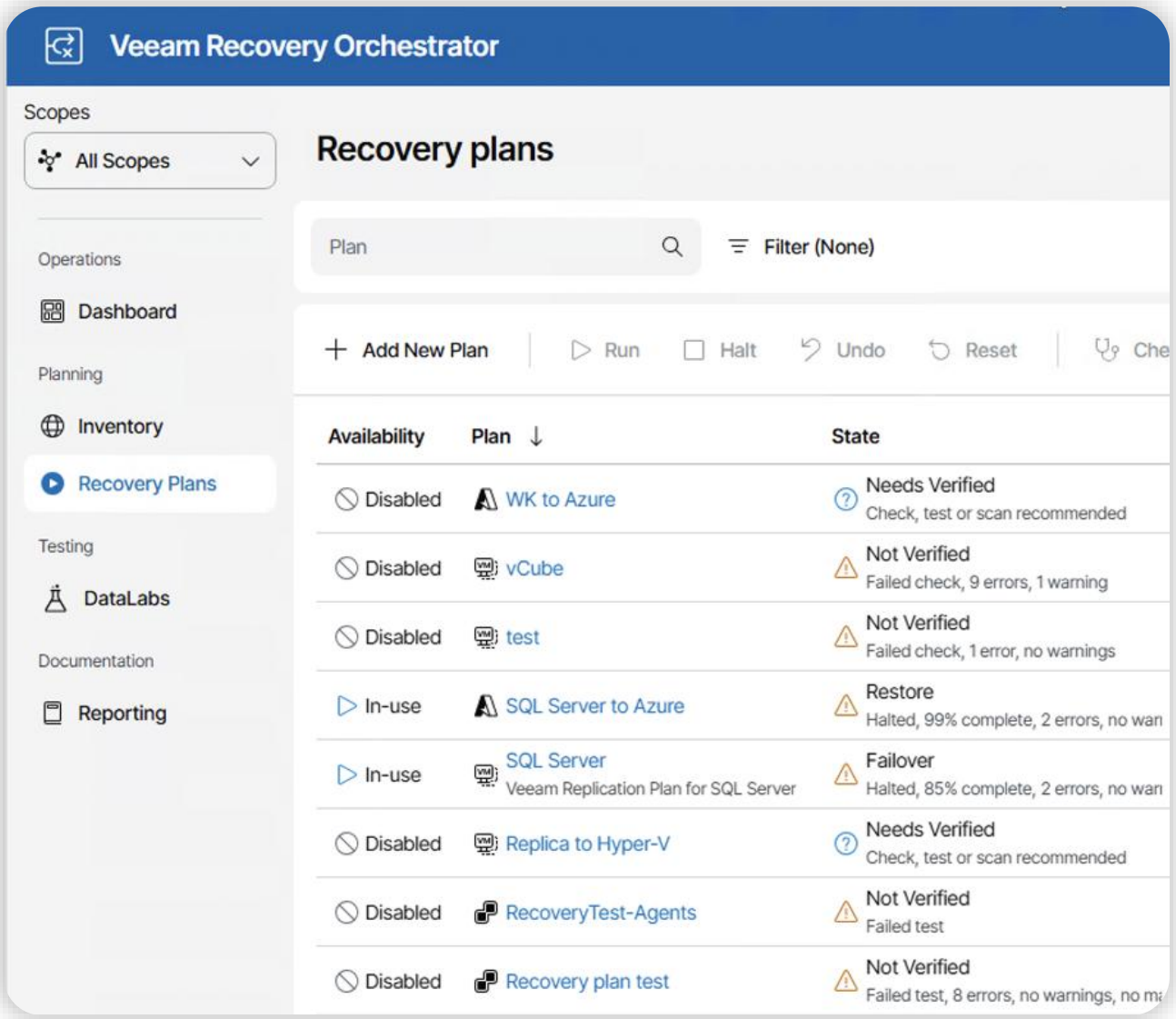
Wiederherstellungs- und Orchestrierungsfehler

Plan erstellen

Definieren Sie Recovery Objectives (RTO und RPO), die den Geschäftsanforderungen entsprechen.

Erfassen Sie kritische Anwendungen, Abhängigkeiten und Infrastrukturkomponenten, umeine vollständige Recovery-Abdeckung sicherzustellen.

Fügen Sie erforderliche Validierungsschritte für Anwendungen und Dienste in den Recovery-Plan ein.



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

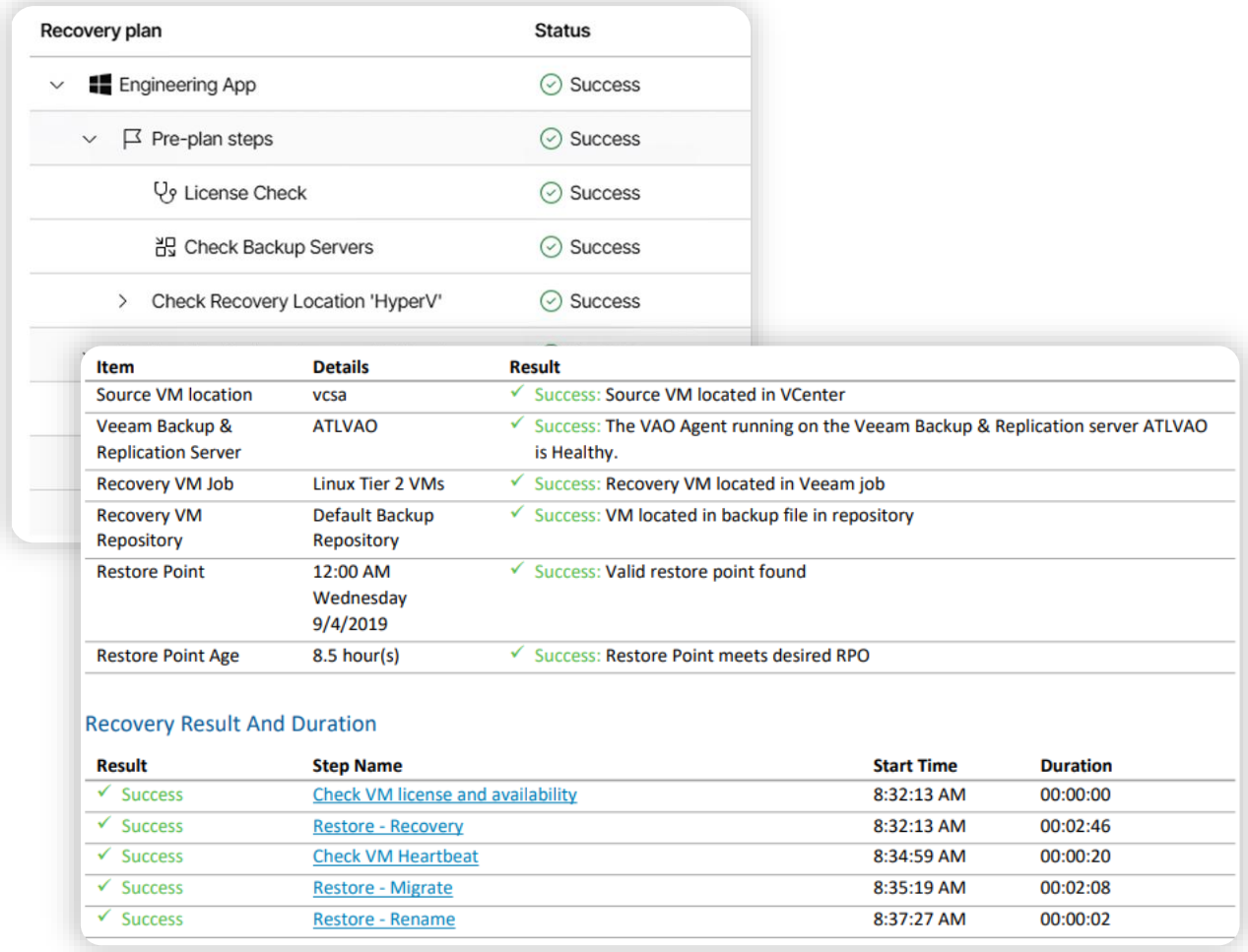
Wiederherstellungs- und Orchestrierungsfehler

Validieren und Testen

Führen Sie automatisierte Recovery-Verifikationstests in isolierten Umgebungen durch, um sicherzustellen, dass Backups ohne Auswirkungen auf die Produktion wiederherstellbar sind.

Erstellen Sie detaillierte Validierungsberichte, die Erfolgsraten, potenzielle Probleme und Verbesserungsbereiche aufzeigen.

Führen Sie regelmäßige, geplante Validierungsübungen durch, um Compliance sicherzustellen und die Bereitschaft für reale Disaster-Recovery-Szenarien aufrechtzuerhalten.



Recovery plan	Status
Engineering App	Success
Pre-plan steps	Success
License Check	Success
Check Backup Servers	Success
Check Recovery Location 'HyperV'	Success

Item	Details	Result
Source VM location	vcsa	Success: Source VM located in VCenter
Veeam Backup & Replication Server	ATLVAO	Success: The VAO Agent running on the Veeam Backup & Replication server ATLVAO is Healthy.
Recovery VM Job	Linux Tier 2 VMs	Success: Recovery VM located in Veeam job
Recovery VM Repository	Default Backup Repository	Success: VM located in backup file in repository
Restore Point	12:00 AM Wednesday 9/4/2019	Success: Valid restore point found
Restore Point Age	8.5 hour(s)	Success: Restore Point meets desired RPO

Recovery Result And Duration

Result	Step Name	Start Time	Duration
Success	Check VM license and availability	8:32:13 AM	00:00:00
Success	Restore - Recovery	8:32:13 AM	00:02:46
Success	Check VM Heartbeat	8:34:59 AM	00:00:20
Success	Restore - Migrate	8:35:19 AM	00:02:08
Success	Restore - Rename	8:37:27 AM	00:00:02

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Entdecken Sie weitere nützliche Ressourcen

Veeam Backup & Replication – Leitfaden für bewährte Sicherheitsverfahren

Liste der Veeam-Sicherheits-Knowledge-Base-Artikel

Bericht zu Ransomware-Trends und proaktiven Strategien 2025

Veeam Cyber Secure Program

Veeam University Free

Veeam University Pro

Veeam Hands-On Labs

© 2025 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

Vielen Dank!