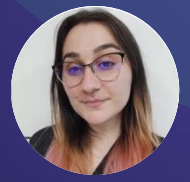
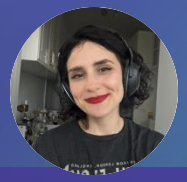
Veeam Data Platform

Sicherheits-Best Practices



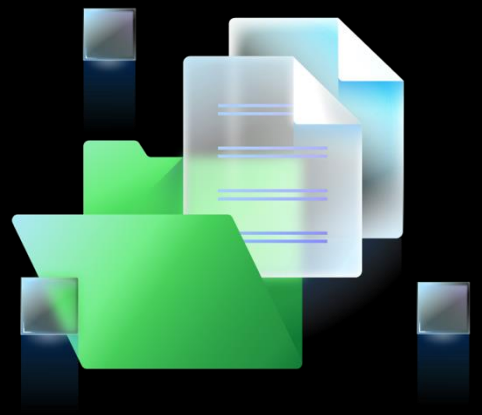
Valentina Ionita
System Engineer



Diana Boro
System 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 manipulierte 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.

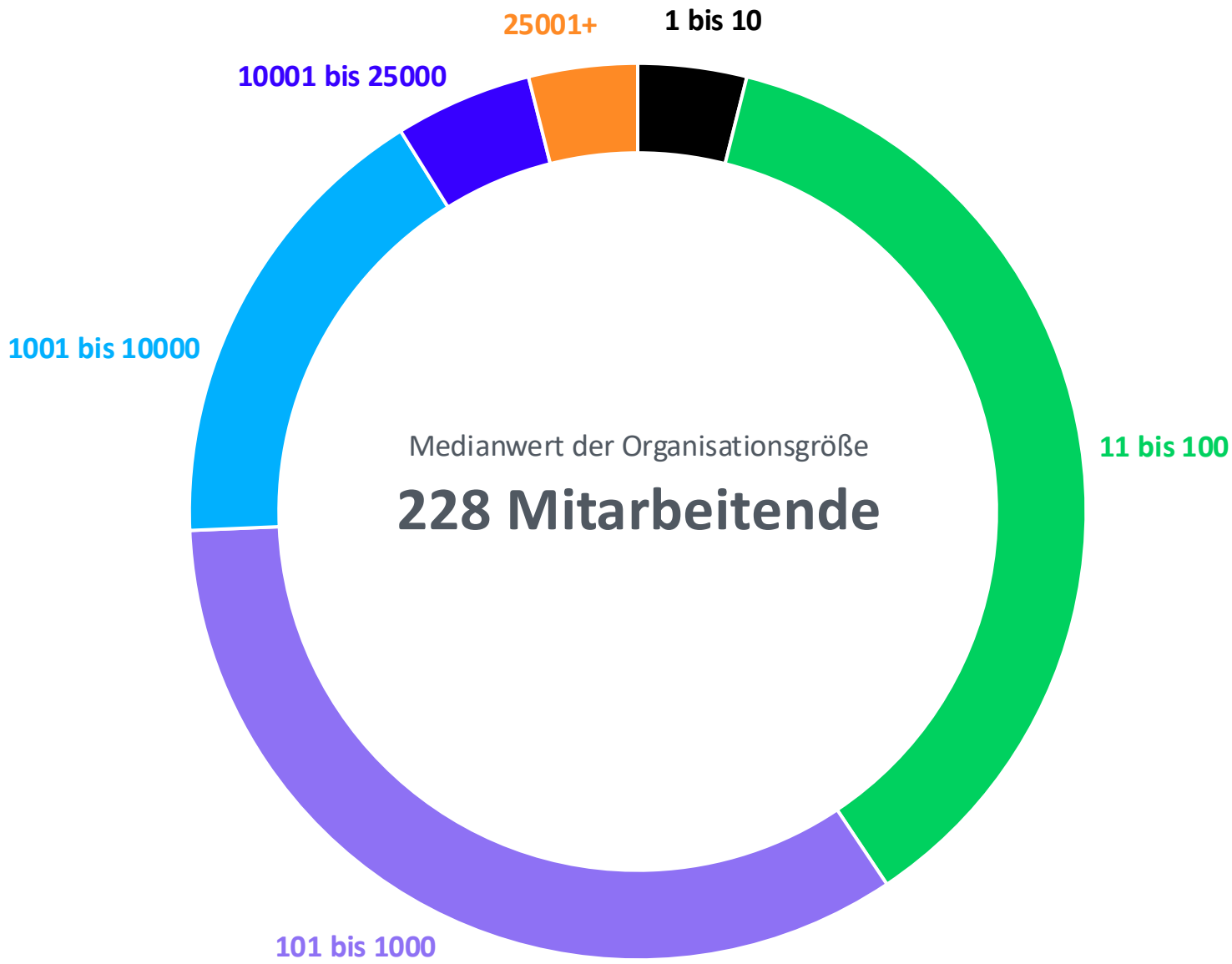
Eine PDF-Version des Foliensets wird Ihnen kurz nach Abschluss dieser Schulung per E-Mail zur Verfügung gestellt. Bitte halten Sie dafür Ihren Posteingang im Blick.

Die Illusion von Sicherheit

69% der Ransomware-Opfer glaubten vor dem Vorfall, gut vorbereitet zu sein – berichteten jedoch nach dem Angriff von einem Rückgang dieses Vertrauens um 20%.

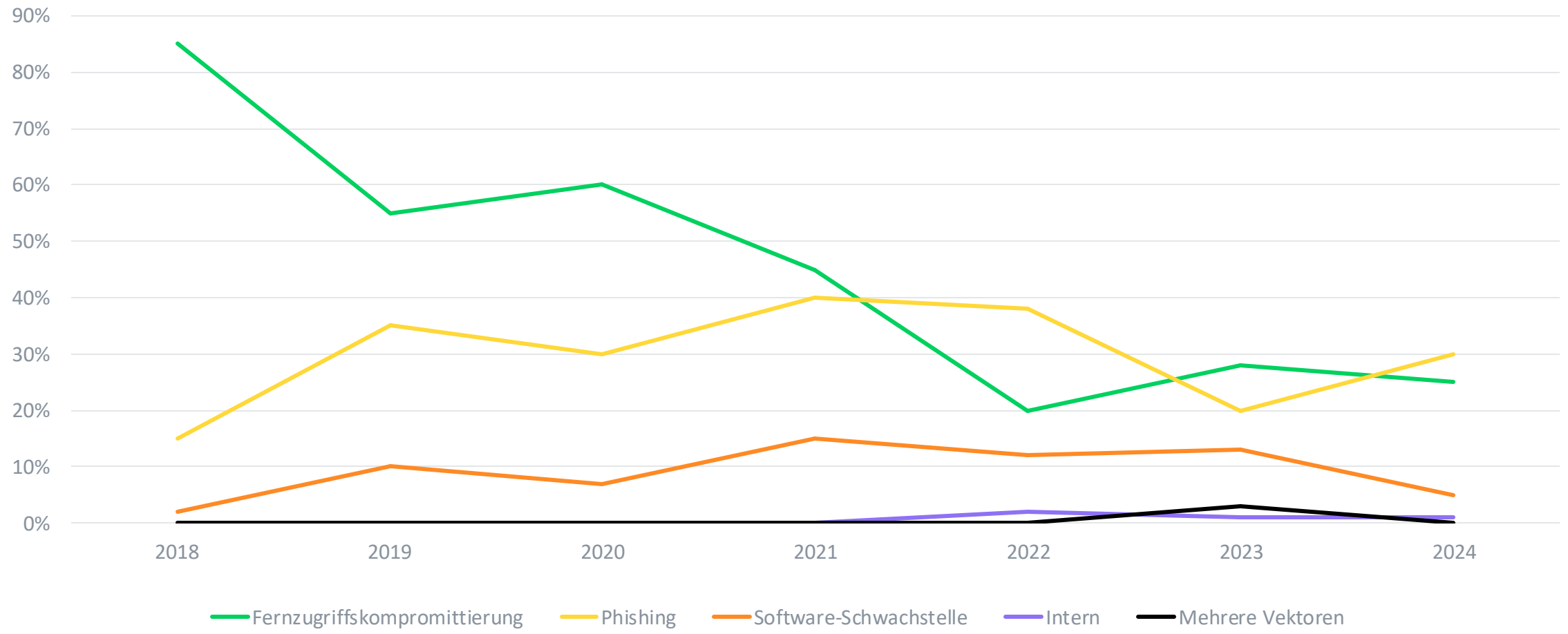
Angriffe können Organisationen jeder Größe treffen.

Von Ransomware betroffene Organisationen nach Mitarbeiterzahl im 1. Quartal 2025



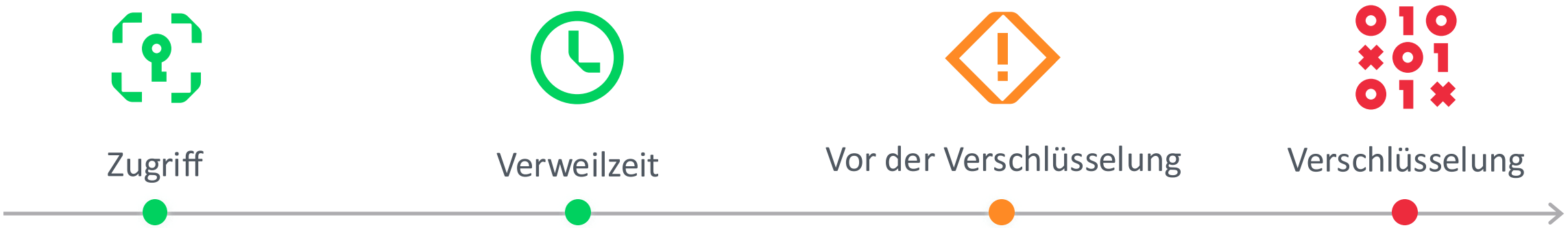
Quelle: https://www.coveware.com/blog/2025/4/29/the-organizational-structure-of-ransomware-threat-actor-groups-is-evolving-before-our-eyes

Wie verschaffen sich Angreifer Zugang?



Quelle: 2025 Ransomware Trends and Proactive Strategies von Veeam - https://go.veeam.com/ransomware-trends

Vereinfachter Zeitablauf von Cyberangriffen



Zugriff

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

Verweilzeit

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

Vor der Verschlüsselung

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

Verschlüsselung

Spät in der Nacht an einem langen Feiertagswochenende beginnt die Verschlüsselung.

Vor welchen Bedrohungen müssen Sie sich schützen?

Infrastruktur-Sicherheit

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

Datensicherheit

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

Betriebssicherheit

- Insider-Bedrohungen
- Fehler bei Wiederherstellung und Orchestrierung

Risiko #1

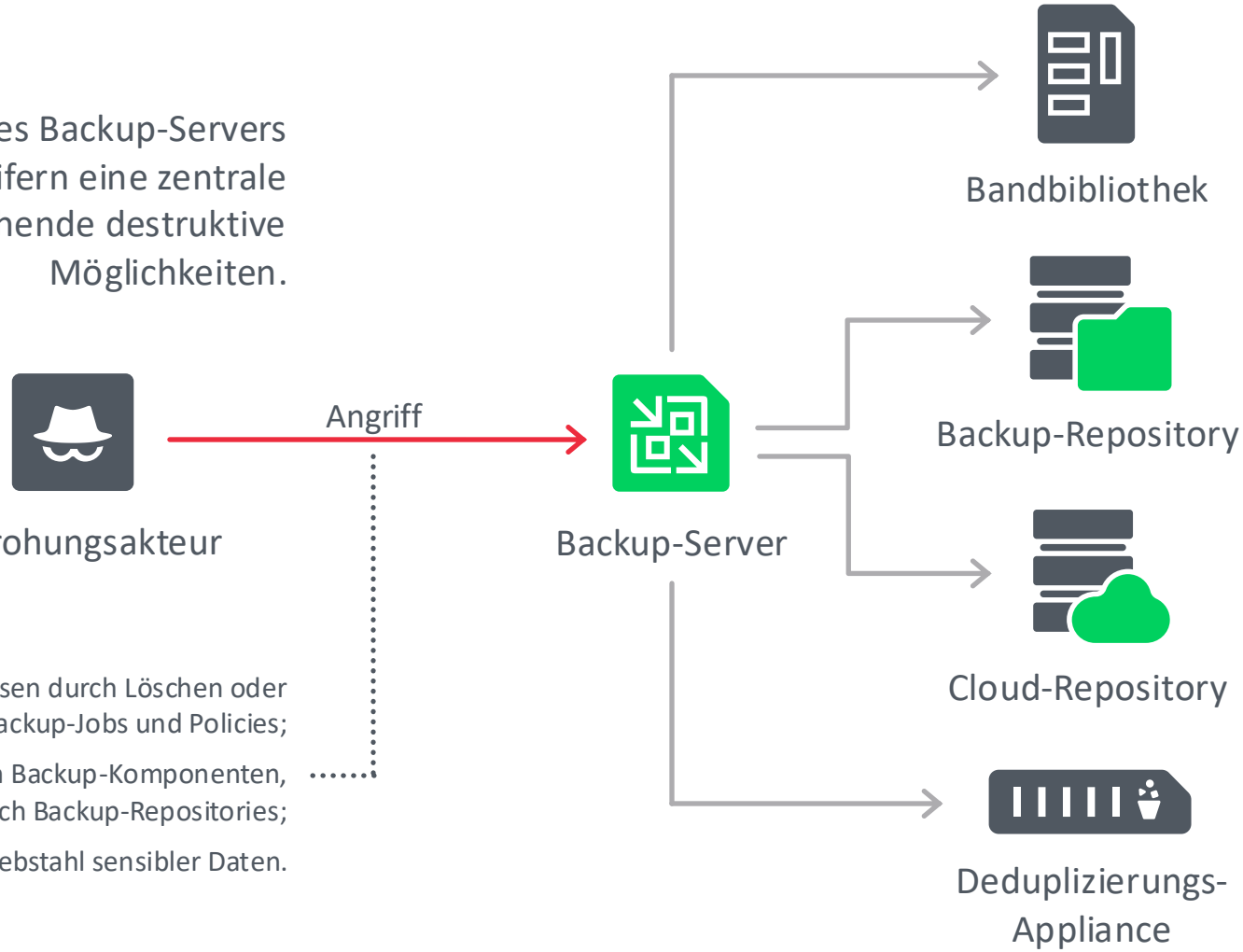
Kompromittierung des Backup-Servers

82% der Fortune-500-Unternehmen nutzen Veeam – dadurch werden Backup-Server zu hochattraktiven Zielen. 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.

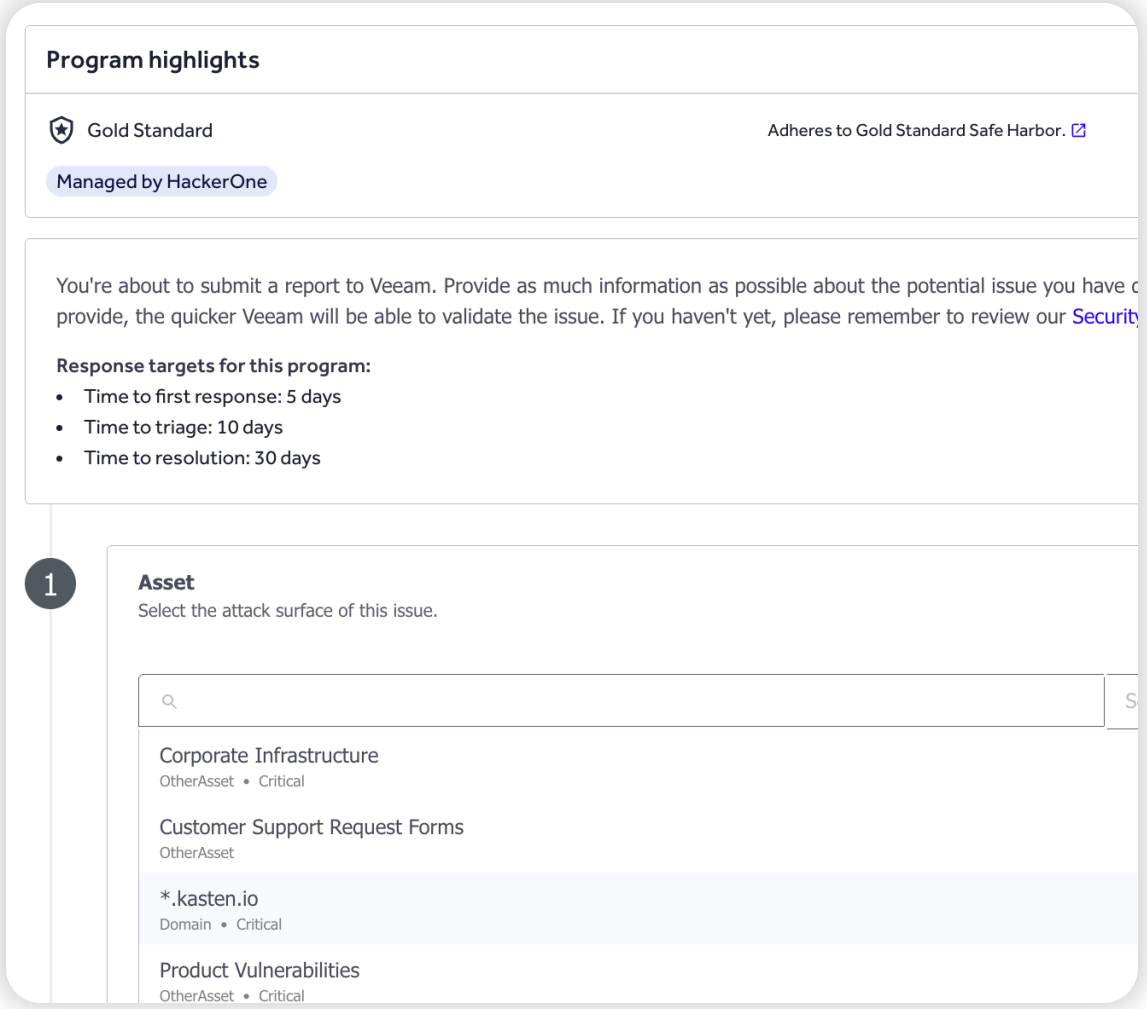
Kompromittierung des Backup-Servers

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.



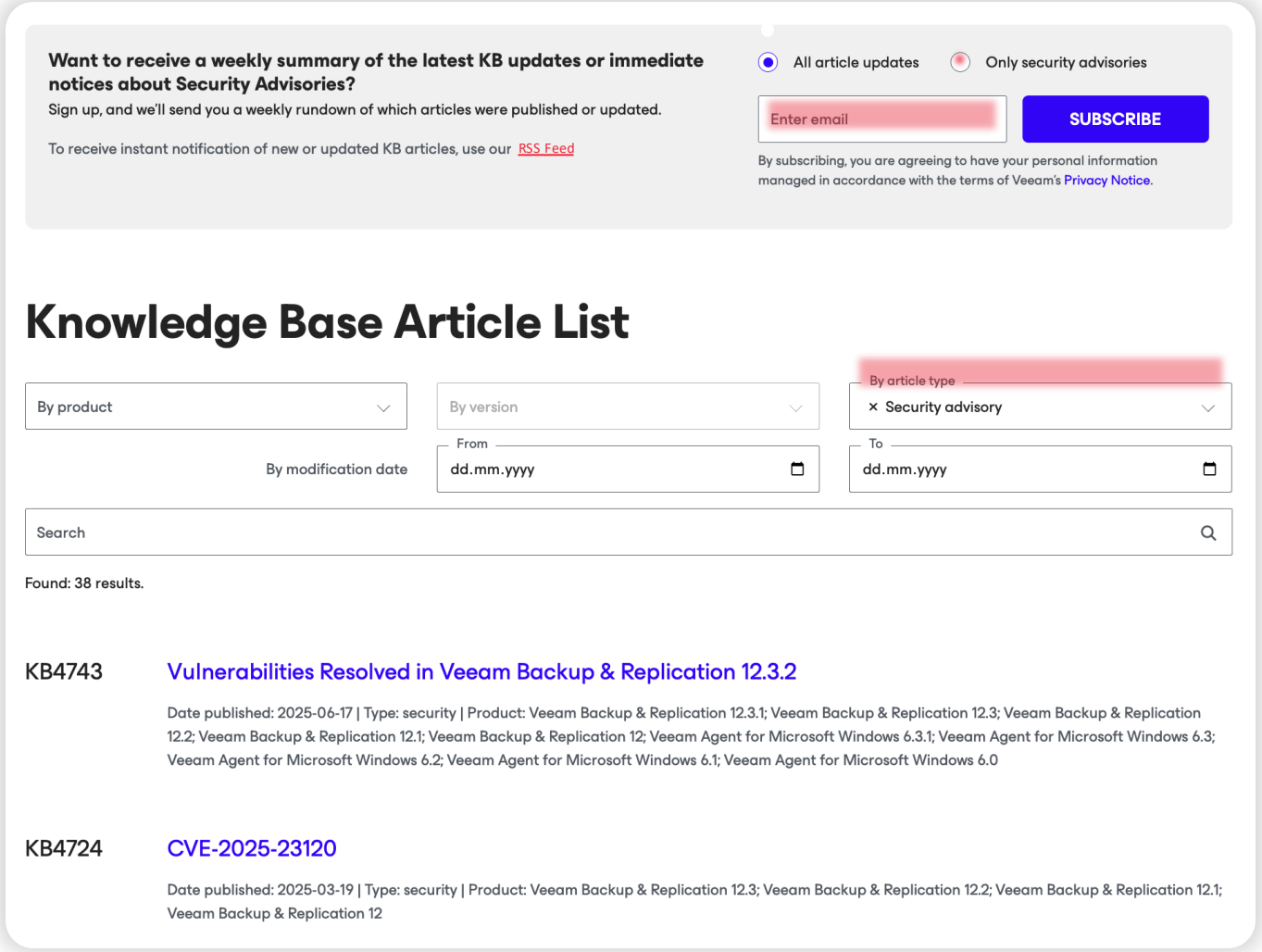
Kompromittierung des Backup-Servers

Stellen Sie sicher, dass Sie stets auf dem aktuellen Stand sind!

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.



Kompromittierung des Backup-Servers

Security & Compliance Analyzer

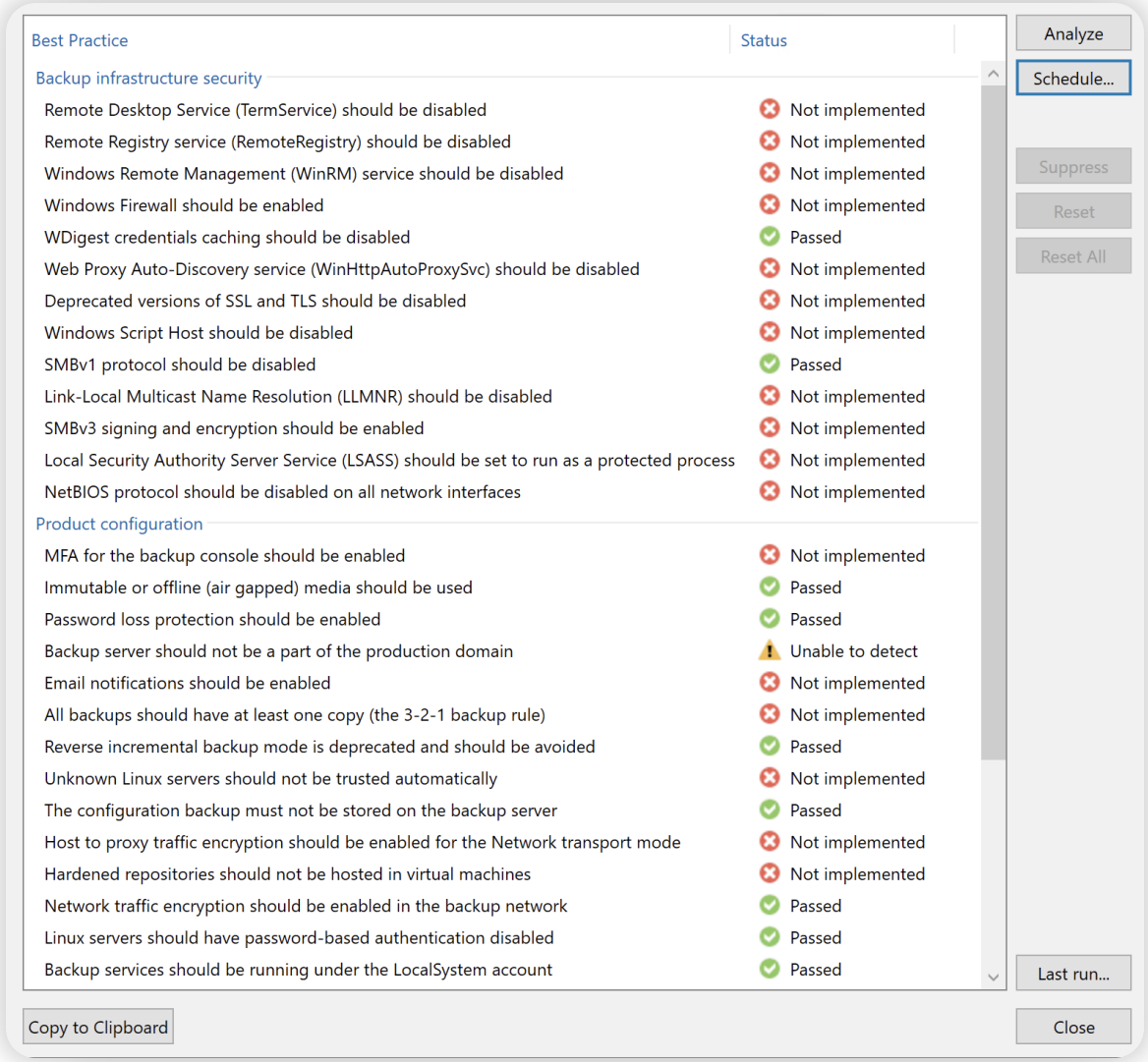
Security & Compliance Analyzer ist eine integrierte Funktion in Veeam Backup & Replication.

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.



Kompromittierung des Backup-Servers

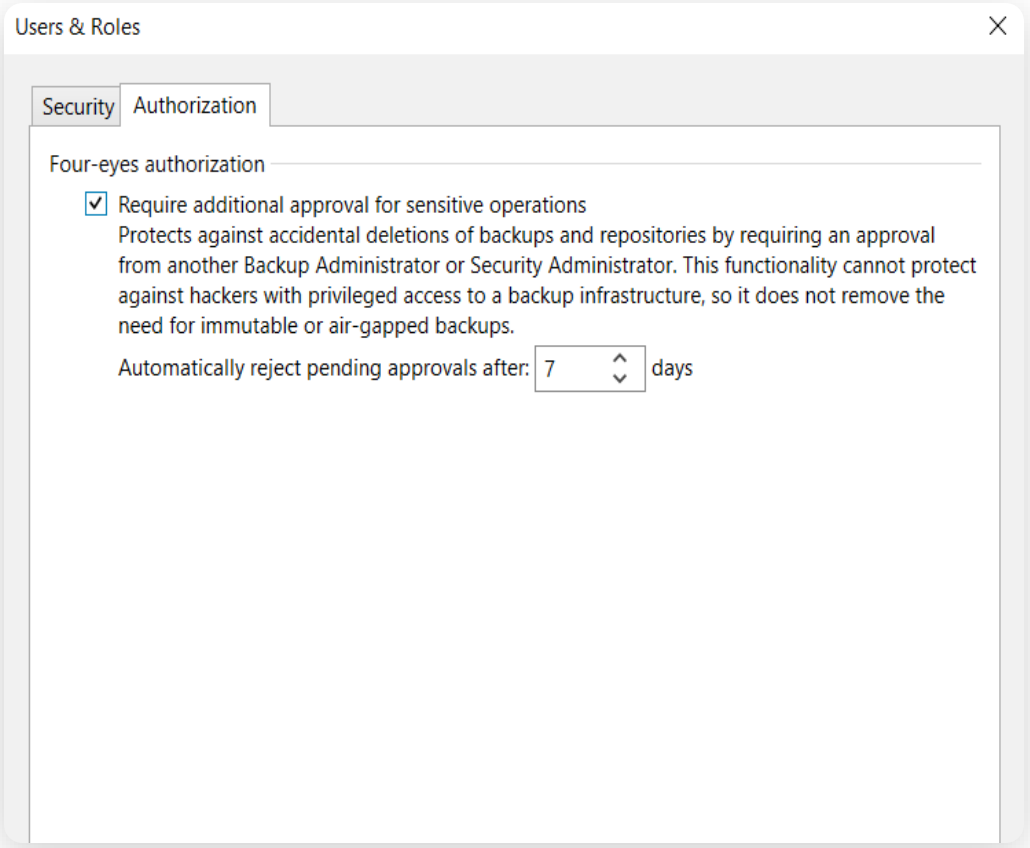
Security & Compliance Analyzer

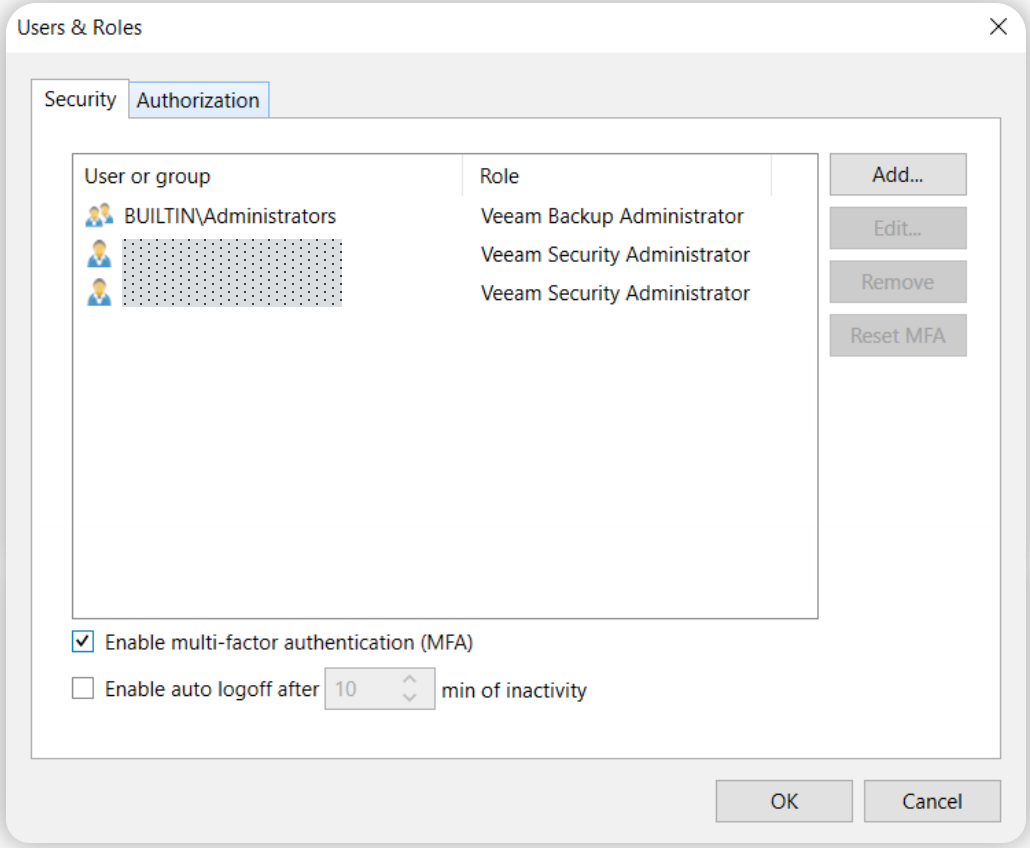
Hier sind einige wirkungsvolle Empfehlungen zur Härtung des Backup-Servers:

- Stellen Sie sicher, dass der Veeam Backup & Replication (VBR)-Server kein Mitglied einer Active-Directory-Domäne ist. Das Betreiben des VBR-Servers in einer Arbeitsgruppe reduziert die Angriffsfläche und begrenzt laterale Bewegungen, falls Domänenanmeldedaten kompromittiert werden.
- Erzwingen Sie MFA für den Zugriff auf die VBR-Konsole. Dies erhöht den Schutz vor unbefugten Anmeldungen erheblich – selbst wenn Zugangsdaten gestohlen oder erraten wurden.
- Aktivieren Sie die Vier-Augen-Autorisierung, bei der zwei autorisierte Personen sensible Vorgänge freigeben müssen.
- Nutzen Sie die „Security Officer“-Funktion (in der Veeam Software Appliance verfügbar). Dies ist eine Rolle, die Anfragen zur Rechteerhöhung und andere sensible Vorgänge genehmigt.
- Deaktivieren Sie RDP, wo immer möglich, oder beschränken Sie den RDP-Zugriff auf den VBR-Server stark. Falls RDP notwendig ist, sollten Sie den Zugriff auf vertrauenswürdige IP-Adressen begrenzen und Network Level Authentication verwenden, um die Angriffsfläche für Brute-Force- und Remote-Attacken zu reduzieren.

Kompromittierung des Backup-Servers

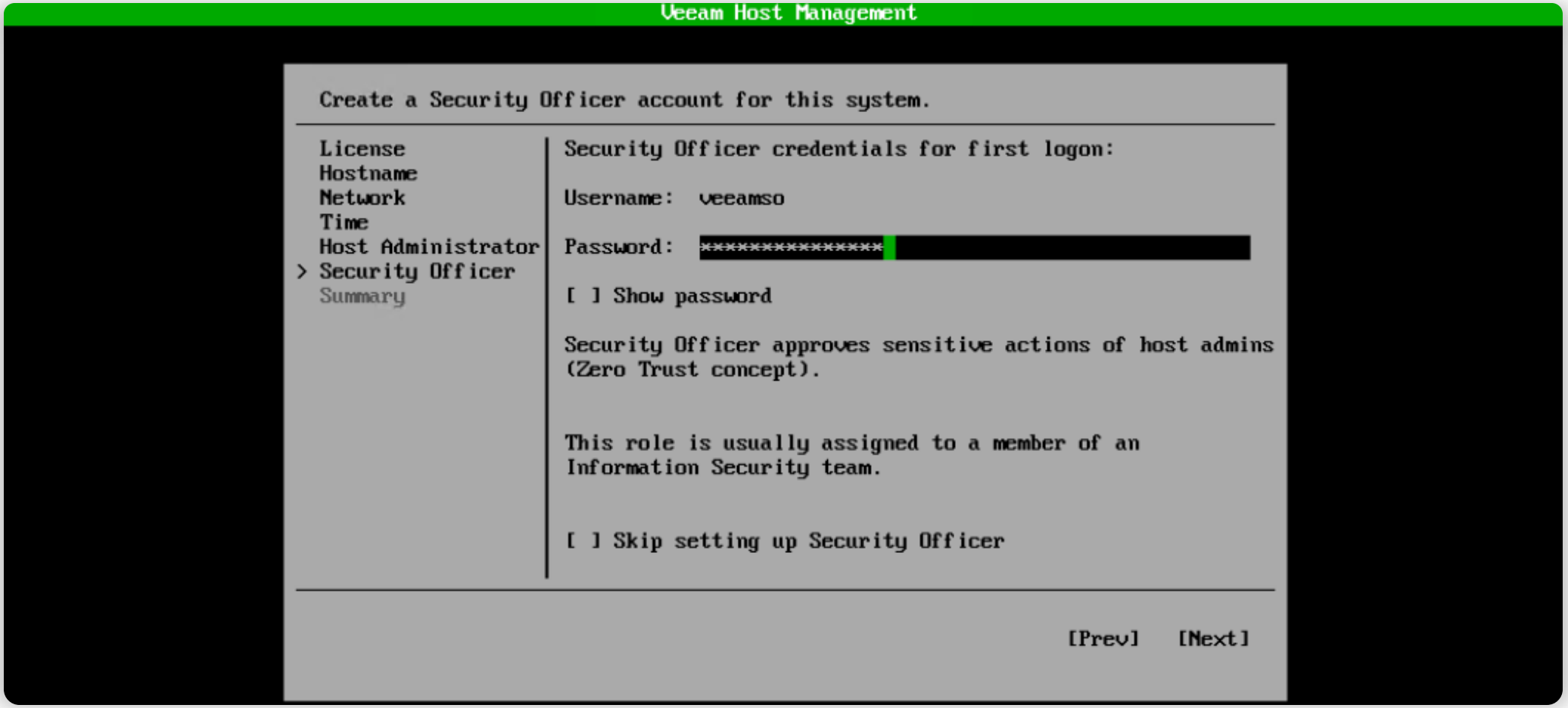
MFA & Vier-Augen-Autorisierung





Kompromittierung des Backup-Servers

Security Officer (Veeam Software Appliance)



Kompromittierung des Backup-Servers

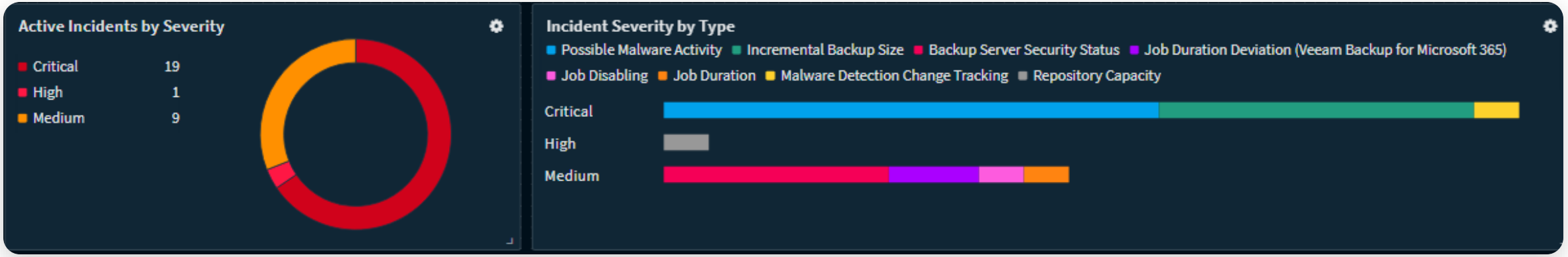
Seien Sie informiert: Security Information & Event Management (SIEM)

10 kritische Alarme, um Ransomware zu stoppen und die Geschäftskontinuität zu schützen

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

- Alarm bei überschrittenen MFA-Versuchen
- Alarm für verdächtige Ransomware-Aktivitäten
- Versuchte Löschvorgänge von Backups
- Erkannte Malware-Aktivität

splunk> CROWDSTRIKE FORTINET paloalto NETWORKS SOPHOS



veeam

Kompromittierung des Backup-Servers

Konfigurations-Backup

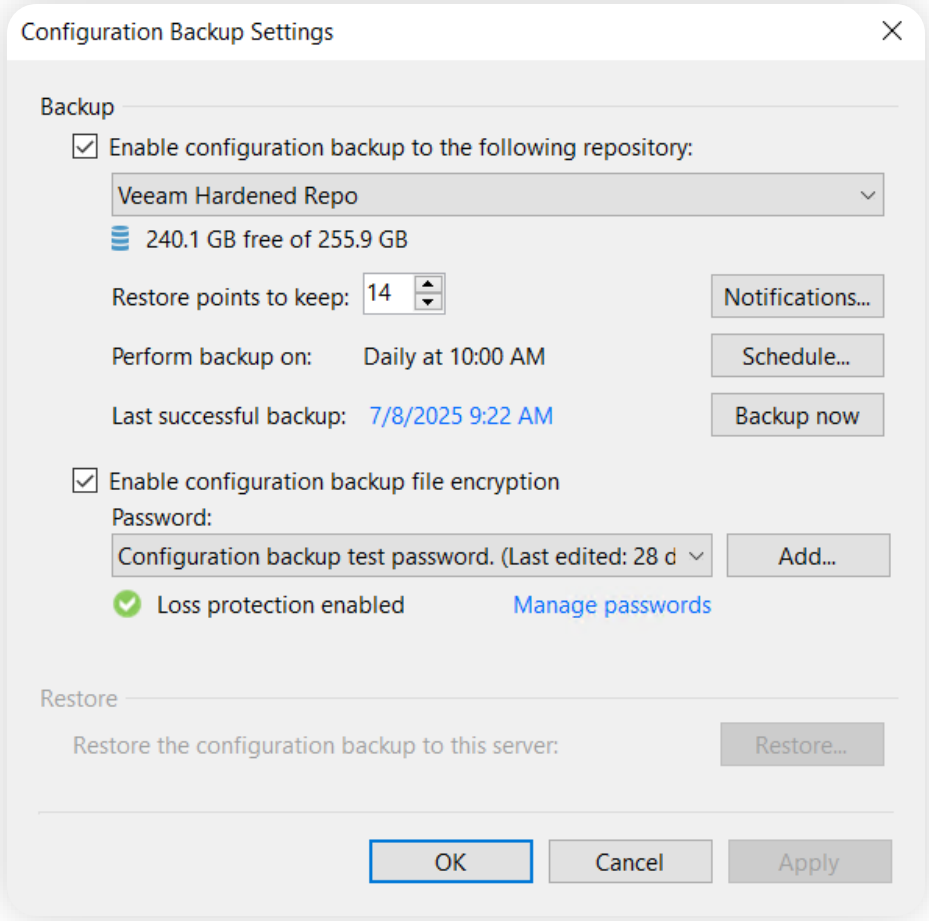
Das Konfigurationsdatenbank-Backup ist die Methode, mit der VBR „sich selbst sichert“.

Verschlüsseln Sie die Daten in den Konfigurations-Backups mit einem sicheren Passwort.

Speichern Sie Konfigurations-Backups an einem sicheren und unveränderbaren Speicherort.

Befolgen Sie das 3-2-1-Backup-Designprinzip.

Planen Sie regelmäßige Konfigurations-Backups ein, um aktuelle Wiederherstellungspunkte sicherzustellen.



Kompromittierung des Backup-Servers

Datenexfiltration

Datenexfiltration ist der unbefugte Diebstahl von Daten aus Backup- oder Produktionsumgebungen.

Angreifer exfiltrieren häufig Daten, bevor sie Ransomware einsetzen, um zusätzlichen Druck auf die Opfer auszuüben – beispielsweise durch die Drohung, gestohlene Informationen zu veröffentlichen oder zu verkaufen, wenn kein Lösegeld gezahlt wird. Diese Vorgehensweise erhöht das Risiko nicht nur von Datenverlust, sondern auch von Datenschutzverletzungen, Reputationsschäden und regulatorischen Sanktionen.

Die Tools Indicators of Compromise Scanner und Threat Hunter können dabei helfen, Hinweise auf Exfiltrationswerkzeuge oder verdächtige Aktivitäten zu identifizieren.

Durch die Verschlüsselung von Backups sowohl während der Übertragung als auch im gespeicherten Zustand stellt Veeam sicher, dass Angreifer die Daten – selbst bei Zugriff oder Abfangen – nicht ohne Weiteres lesen oder missbrauchen können.

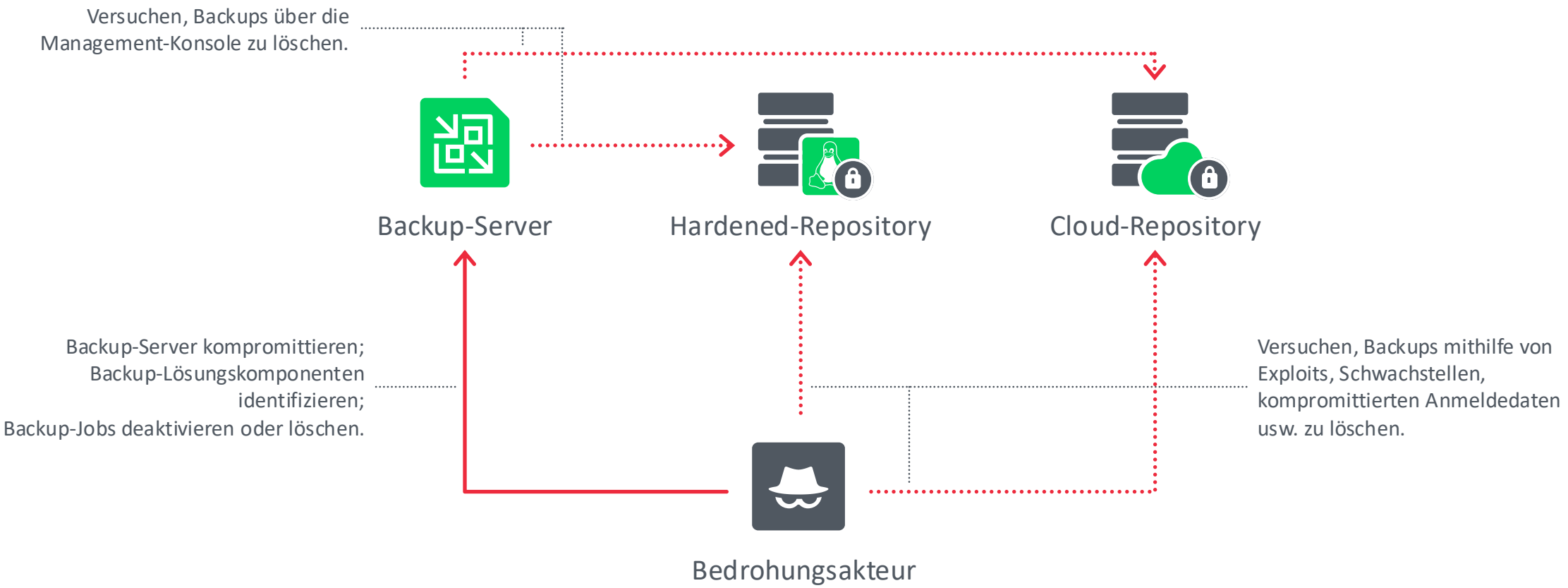
Risiko #2

Verschlüsselung/Löschung von Backupdateien

Statistik: 89% der Organisationen hatten Angriffe auf ihre Backup-Repositories, und mehr als ein Drittel erlebte, dass kritische Backup-Daten verändert oder zerstört wurden.

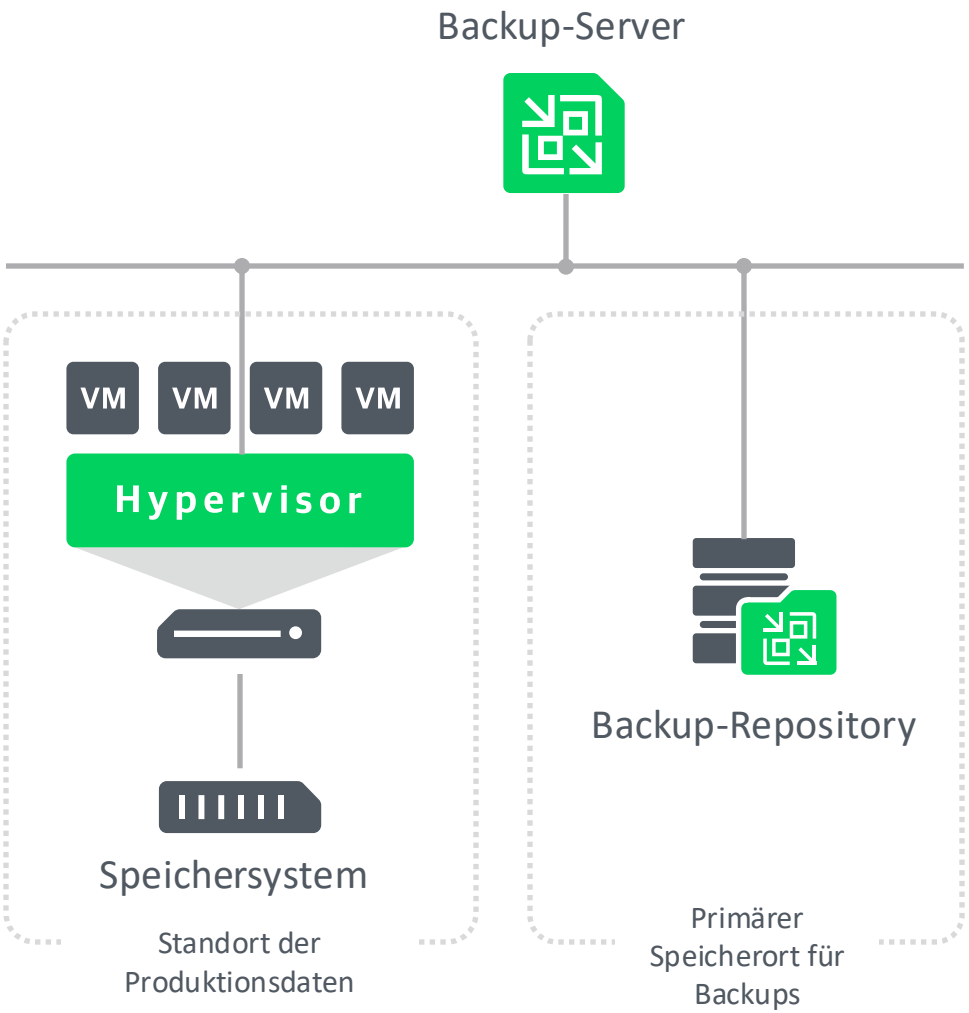
Verhinderung der Verschlüsselung bzw. Löschung von Backupdateien

Resilienz-Domänen



Verhinderung der Verschlüsselung bzw. Löschung von Backupdateien

3-2-1-Regel

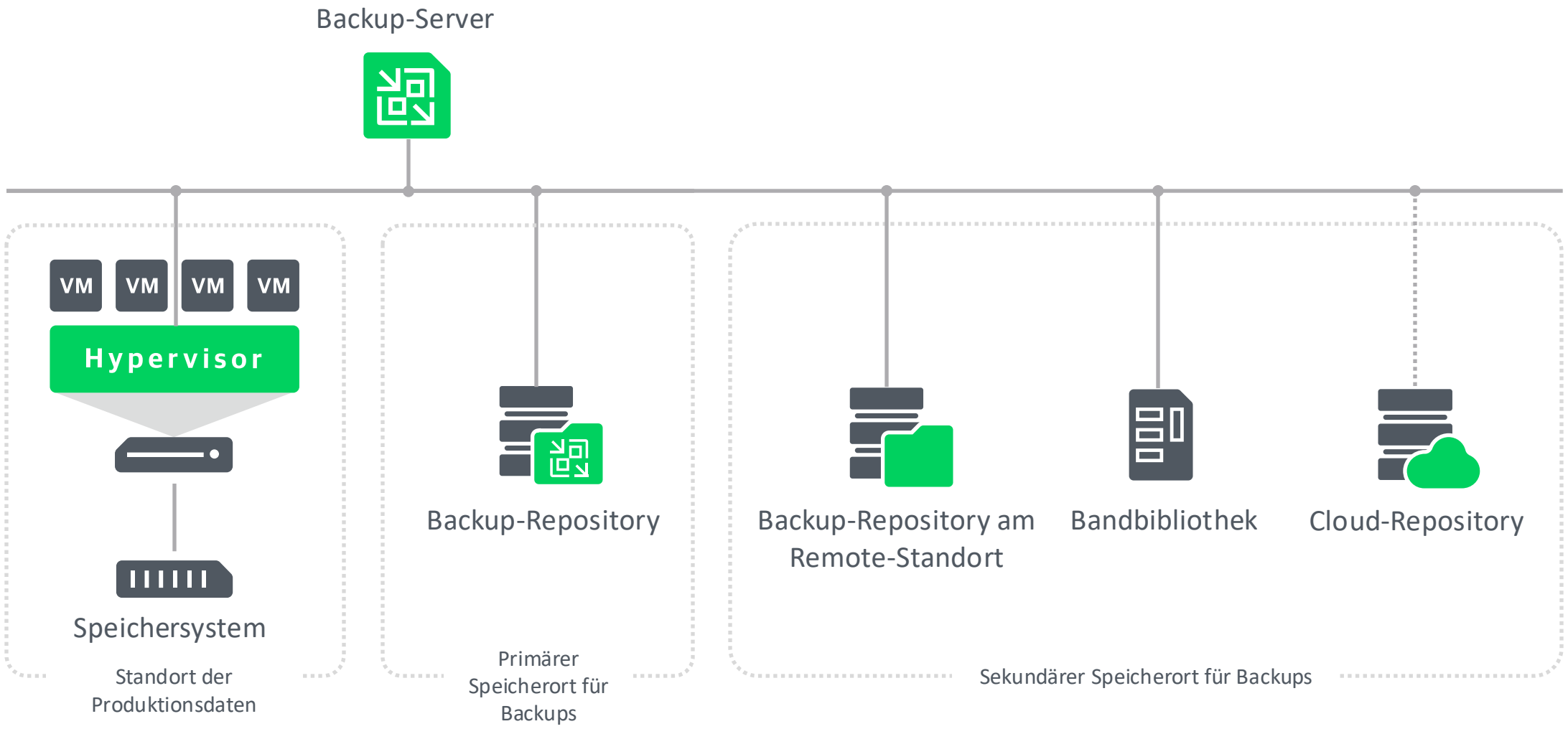


Durch das Vorhalten mehrerer Kopien auf unterschiedlichen Medientypen und mindestens einer externen Kopie stellt diese Regel sicher, dass es keinen Single Point of Failure gibt und Datenverlust deutlich unwahrscheinlicher wird.

Geht eine Kopie aufgrund von Hardwarefehlern, Bedienfehlern oder eines Cyberangriffs verloren, beschädigt oder kompromittiert, stehen weiterhin andere Kopien zur Wiederherstellung zur Verfügung.

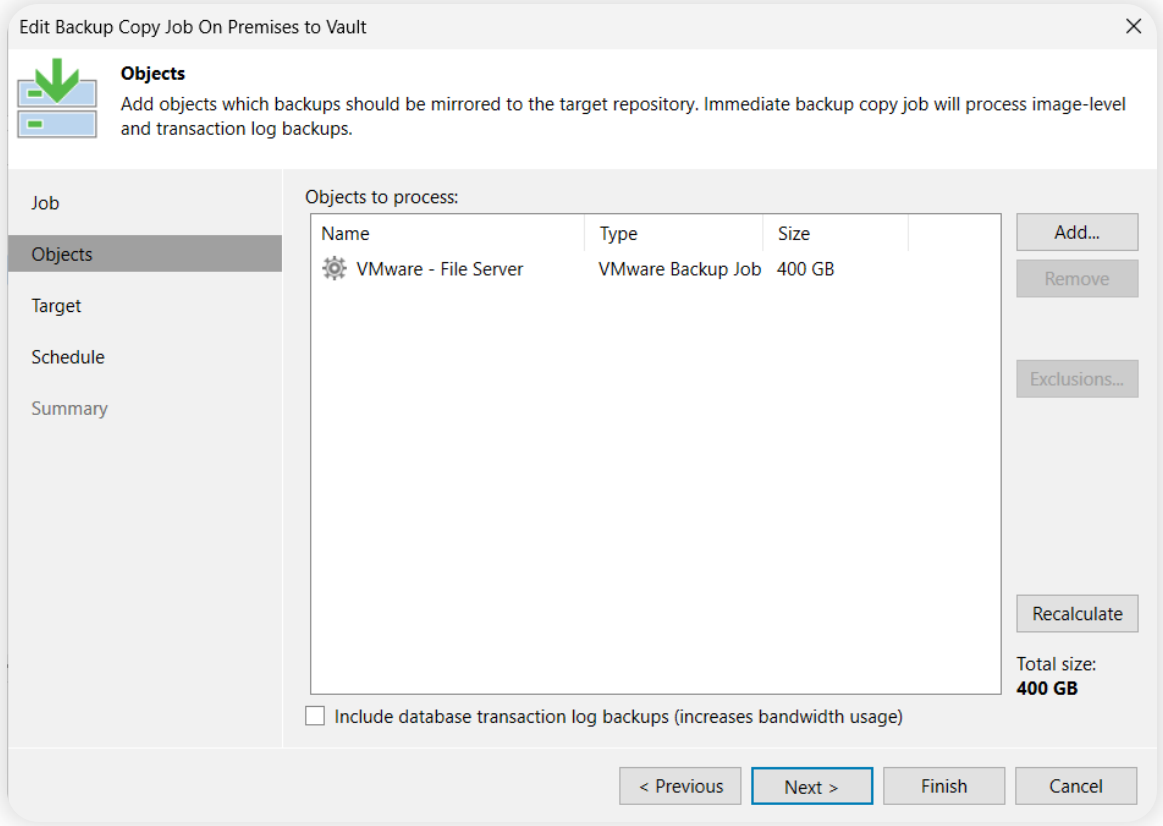
Verhinderung der Verschlüsselung bzw. Löschung von Backupdateien

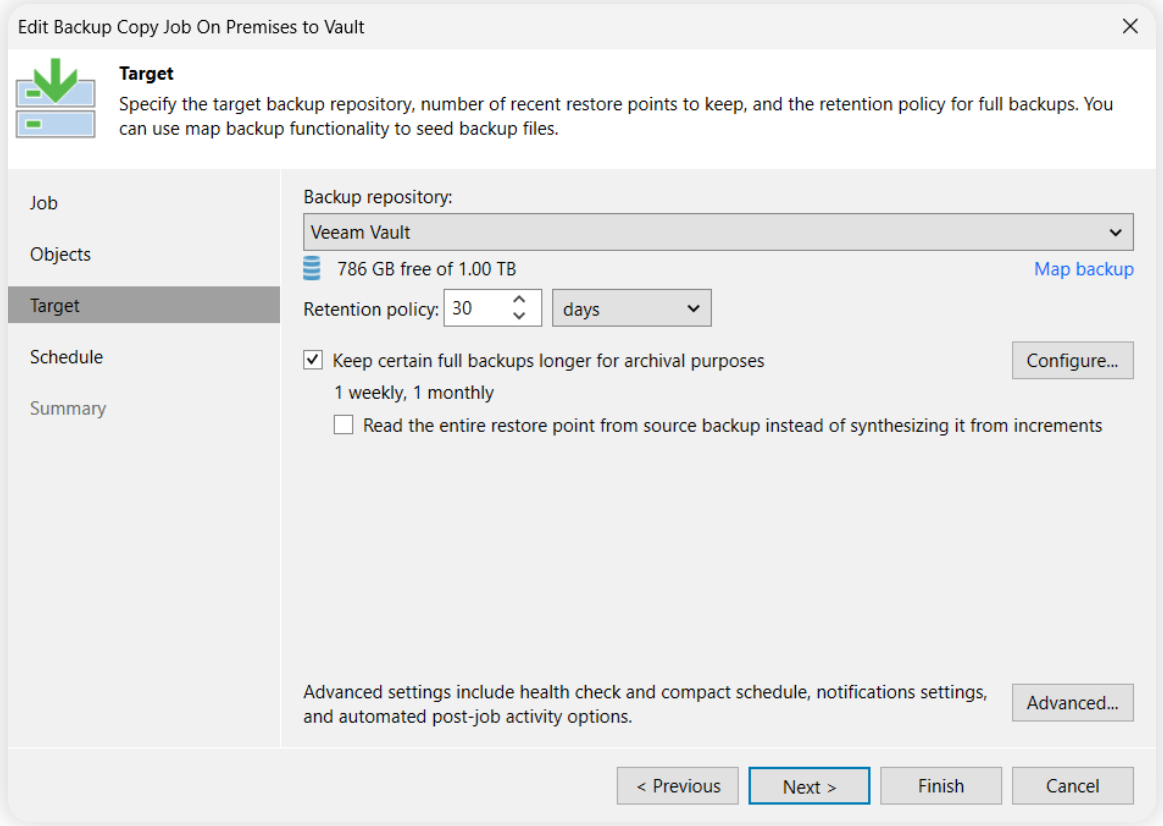
3-2-1-Regel



Verhinderung der Verschlüsselung bzw. Löschung von Backupdateien

Backup-Copy-Job





Verhinderung der Verschlüsselung bzw. Löschung von Backupdateien

Unveränderbarkeit

Definition von Unveränderbarkeit:

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

Vorteile der Unveränderbarkeit:

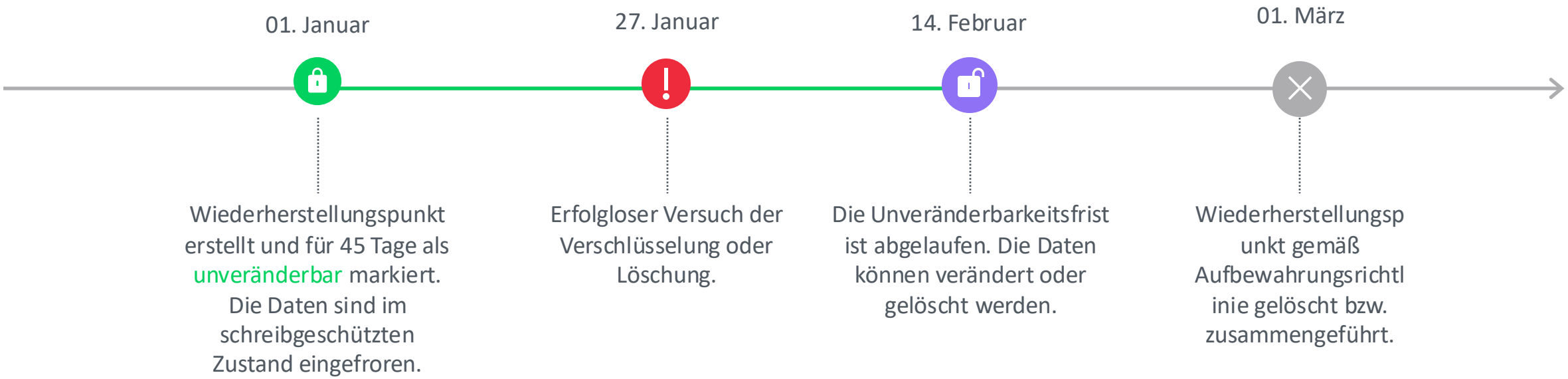
- Stellt die Datenintegrität und -sicherheit sicher.
- Bietet Schutz vor Ransomware und unbeabsichtigten Löschvorgängen.

Unterstützte Typen unveränderbarer Repositories

- Veeam Hardened Repository
- Veeam Data Cloud Vault
- Amazon-, Azure-, Google-Cloud-Storage und andere S3-kompatible Object-Storage-Repositories
- HPE StoreOnce
- Dell EMC Data Domain

Verhinderung der Verschlüsselung bzw. Löschung von Backupdateien

Zeitleiste der Unveränderbarkeit



Verhinderung der Verschlüsselung bzw. Löschung von Backupdateien

Hardened Repository

Ein Hardened Repository ist ein sicherer Speicher mit Unveränderbarkeit-Unterstützung, der darauf ausgelegt ist, Sicherungsdaten vor Löschung, Veränderung oder Angriffen (wie Ransomware) zu schützen – selbst dann, wenn jemand unautorisierten Zugriff erlangt.

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

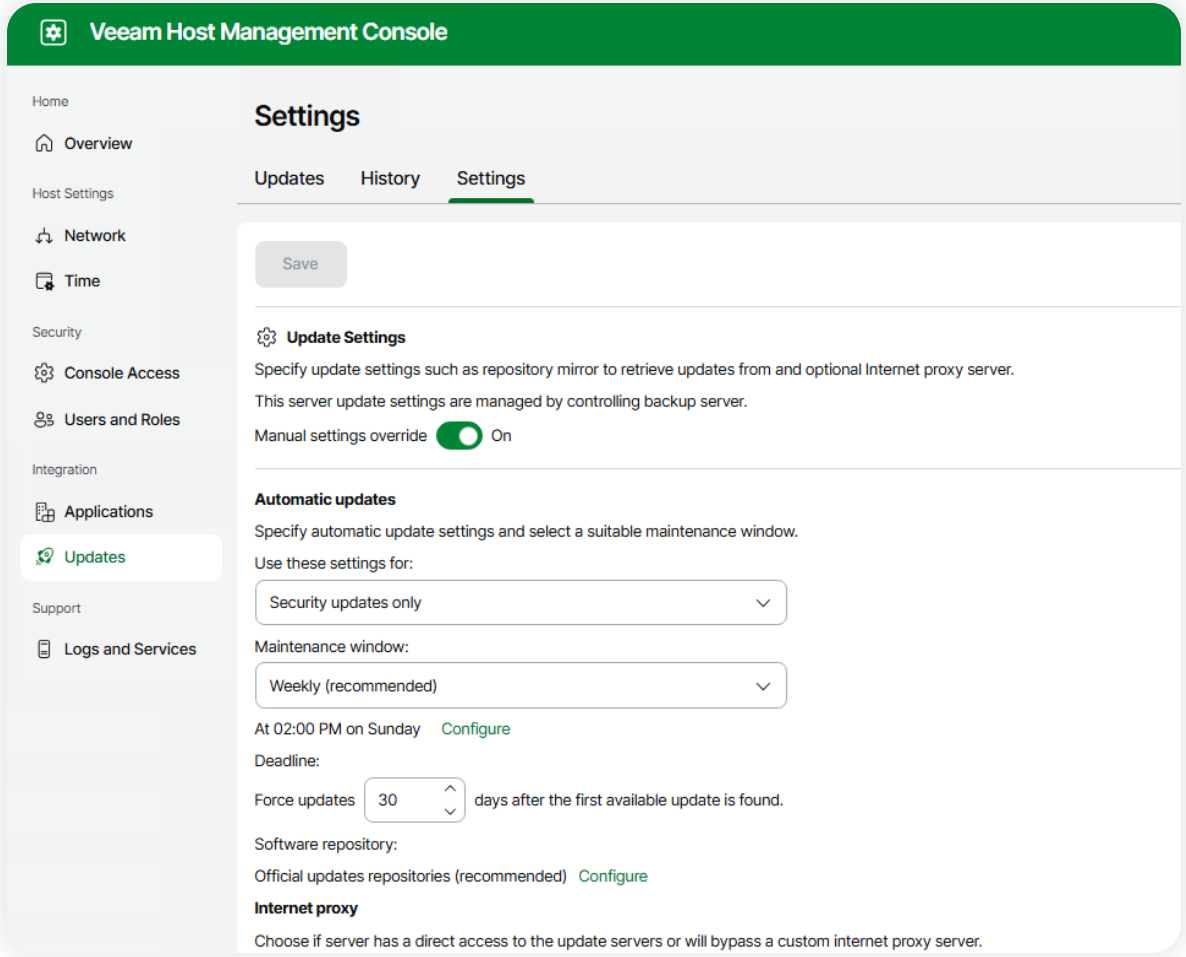
  Die Maschine muss die Systemanforderungen für Backup-Repositorys erfüllen; für das gehärtete Repository gelten zusätzliche Anforderungen und Einschränkungen.

- Kann über das von Veeam bereitgestellte Hardened Repository ISO installiert werden (JeOS + Repository-Pakete). JeOS verwaltet und aktualisiert das Betriebssystem und die Veeam-Komponenten und vereinfacht so die Wartung durch automatische Updates.

  Hardware muss auf der Red-Hat-Kompatibilitätsliste oder der CIQ-zertifizierten Hardwareliste stehen.

Verhinderung der Verschlüsselung bzw. Löschung von Backupdateien

JeOS Host Management Console



- Angepasste Version von minimalem Rocky Linux
- Einfache und schnelle Bereitstellung
- Vorab gehärtet mit dem DISA-STIG Security Profile
- Vollständig automatisierte Schwachstellen-Patches
- MFA ist obligatorisch

Verhinderung der Verschlüsselung bzw. Löschung von Backupdateien

Funktionen des Hardened Repository

- Unveränderbare Backups: Dateien sind für einen vom Benutzer definierten Zeitraum vor Änderung und Löschung geschützt – selbst dann, wenn administrative Anmeldedaten kompromittiert werden. Dadurch können Backups weder durch Malware, Ransomware noch durch versehentliche Administratoraktionen verändert oder gelöscht werden.

- Air-gapped-ähnlicher Schutz: Das Repository wird gehärtet, indem der Zugriff eingeschränkt und Protokolle wie SSH deaktiviert werden. Dies reduziert die Angriffsfläche und macht das Repository zu einer „undurchdringlichen Blackbox“ für Backupdateien.

- Schutz vor Insiderbedrohungen: Durch den Einsatz von Einmal-Anmeldedaten und das Deaktivieren des Root-Zugriffs für Backup-Vorgänge werden Risiken minimiert – selbst wenn der zentrale Veeam-Server kompromittiert wird.

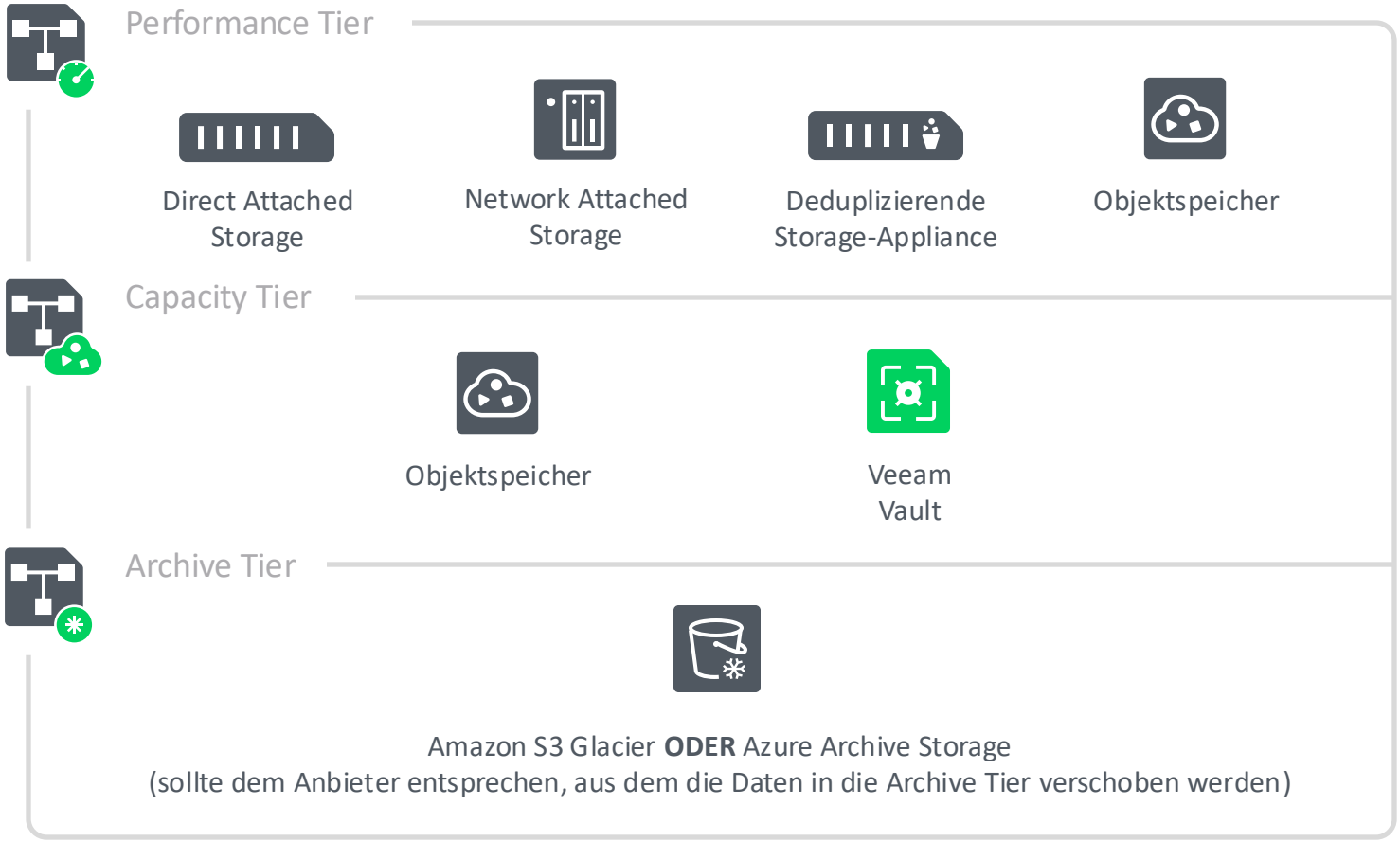
- Speichereffizienz: In Kombination mit dem XFS-Dateisystem profitiert das Repository von der Block-Cloning-Technologie, die effiziente synthetische Voll-Backups, geringeren Speicherverbrauch und schnellere Backup-Vorgänge ermöglicht.

Verhinderung der Verschlüsselung bzw. Löschung von Backupdateien

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.



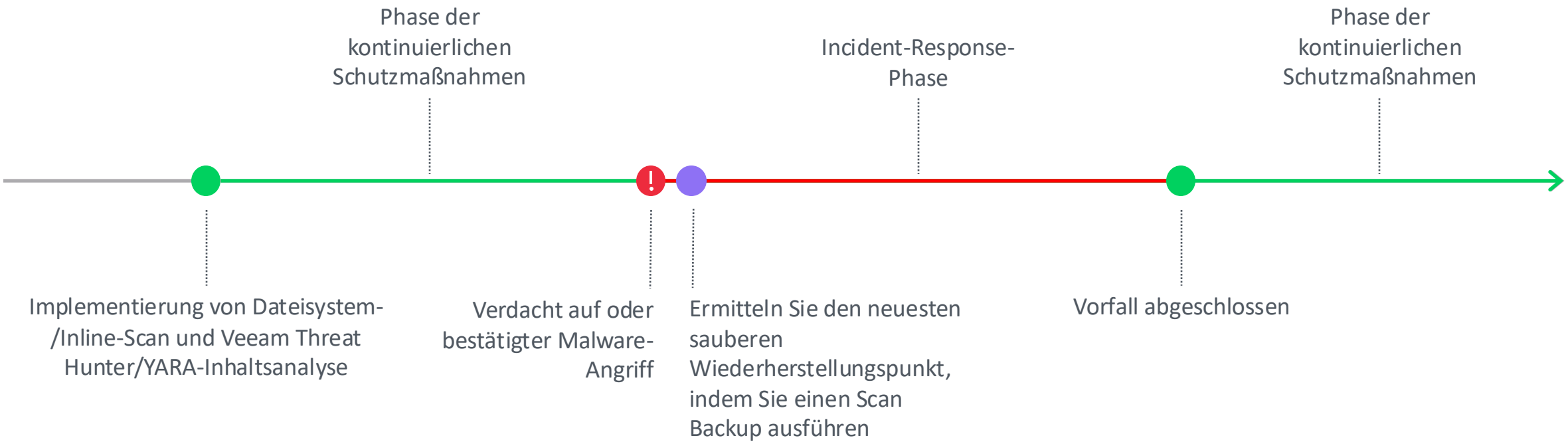
Risiko #3

Malware in Backups

Die Wiederherstellung aus einem infizierten Backup kann Malware erneut in die Produktionsumgebung einschleusen, was zu wiederkehrenden Infektionszyklen und möglicher Datenkorruption in Systemen führt.

Malware in Backups

Vereinfachter Workflow



Malware in Backups

Wie erkennt man Malware?

Analyse der Dateisystemaktivität – wird während des Backup-Jobs genutzt und prüft Gastindexierungsdaten auf: bekannte verdächtige Dateien und Erweiterungen, gelöschte Dateien, Änderungsereignisse bei Dateierweiterungen.

Indicators of Compromise Tools Scanner – Indikatoren für Kompromittierung sind keine Malware, aber ihre unerwartete Präsenz auf einem System kann auf ein Sicherheitsrisiko hinweisen.

Inline Scan (Entropieanalyse) – analysiert Blöcke im Datenstrom während des Backup-Jobs auf: durch Malware verschlüsselte Dateien, durch Malware erzeugte Artefakte wie Onion-Links, Hinweise wie jene von Medusa oder Clop.

Marks infected objects. Signaturbasierte Erkennung (Veeam Threat Hunter) – kann während Scan Backup, Secure Restore und SureBackup genutzt werden. Eine Alternative zu Drittanbieter-Antivirus, die in VBR integriert werden kann. Die Verwendung einer signaturbasierten Engine in der Produktionsumgebung und einer zweiten (Veeam Threat Hunter) mit einem anderen Satz von Malwaredefinitionen für Backups ist eine gute Praxis. Markiert infizierte Objekte.

Regelbasierte Erkennung (YARA) – ähnlich wie die signaturbasierte Erkennung; kann ebenfalls bei Scan Backup, Secure Restore und SureBackup eingesetzt werden. Ermöglicht das Erstellen eigener Regeln zur Identifizierung von Malware anhand textueller oder binärer Muster. Markiert infizierte Objekte.

Drittanbieterlösungen – über die Veeam Incident API ist es möglich, bei erkannter Malwareaktivität eine Meldung an Veeam Backup & Replication zu senden und eine Maschine als infiziert zu markieren.

Malware in Backups

Wann und wie sollten diese Funktionen verwendet werden?

Wann?	Während des Backup-Jobs		On-demand	Vor der Wiederherstellung	Während der Backup-Wiederherstellungsverifikation
Was?	Guest Indexing Data Scan	Inline Scan	Scan Backup	Secure Restore	SureBackup
Wie?	Dateisystem-Aktivitätsanalyse. Scannt Guest-Indexing-Daten nach bekannten verdächtigen Dateien und Erweiterungen, gelöschten Dateien, Erweiterungsänderungen sowie nach Nicht-Malware-Programmen, die ein Sicherheitsrisiko darstellen können (Indicators of Compromise Tools Scanner).	Entropieanalyse. Scannt Datenblöcke im Datenstrom während des Backup-Jobs, z. B. nach durch Malware verschlüsselten Dateien, von Malware erzeugten Artefakten wie Onion-Links sowie Notizen, die von Medusa und Clop erstellt wurden.	Eine signaturbasierte Erkennung (Veeam Threat Hunter) und/oder eine regelbasierte Erkennung (YARA Scan) kann nach einem Malware-Angriff genutzt werden, um den neuesten sauberen Wiederherstellungspunkt zu finden oder sensible Daten im Backup zu identifizieren.	Veeam Threat Hunter und/oder YARA Scan kann verwendet werden, um Maschinendaten auf Malware-Aktivitäten zu prüfen, bevor die Maschine in die Produktionsumgebung zurückgeführt wird.	Veeam Threat Hunter und/oder YARA Scan kann während des SureBackup-Jobs eingesetzt werden, um proaktiv das Risiko zu reduzieren, kompromittierte Daten in die Produktionsumgebung zurückzubringen.

Malware in Backups

Warum wird Veeam Threat Hunter gegenüber einem Antivirenprodukt eines Drittanbieters empfohlen?

- Wird automatisch auf jedem Mount-Server installiert
- 3- bis 6-mal schneller als Windows Defender
- Verwendet Signaturen, die speziell für Backups optimiert sind
- Ähnlicher CPU- und RAM-Verbrauch wie klassische AV-Lösungen – trotz deutlich höherem Durchsatz
- Proprietäre Engine ohne vom Benutzer veränderbare Signaturen
- In Veeam Data Platform Advanced enthalten – keine zusätzlichen AV-Lizenzkosten

Der Wechsel zu einer Antivirenlösung eines Drittanbieters ist jederzeit möglich, wenn Sie dies wünschen.

Malware in Backups

Was ist YARA und wie erstellt man YARA-Regeln?

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

```
rule RuleName {
    meta:
        author = "Security Team"
        description = "Custom threat detection"
        date = "2025-09-04"

    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)
}
```

Malware in Backups

Wo findet man sofort einsetzbare YARA-Regeln?

Öffentliche Repositories

Es gibt zahlreiche community-getriebene Repositories, von denen einige sehr häufig aktualisiert werden. Einfach im Internet suchen oder Ihre bevorzugte KI fragen.

Einige Hinweise:

- Nicht alle öffentlichen Regeln entsprechen denselben Qualitätsstandards. Organisationen sollten Regeln sowohl an schädlichen Samples als auch an sauberen Dateien validieren, um Fehlalarme vor der Nutzung zu minimieren.
- Komplexe Regeln mit vielen Bedingungen können die Scan-Performance deutlich verlangsamen. Beispielsweise sollten Regeln kurze Strings (unter 4 Byte) vermeiden, Wildcards in Hex-Strings minimieren und Regex nur sparsam und mit festen 4-Byte-Ankern verwenden.

Generatoren und LLMs

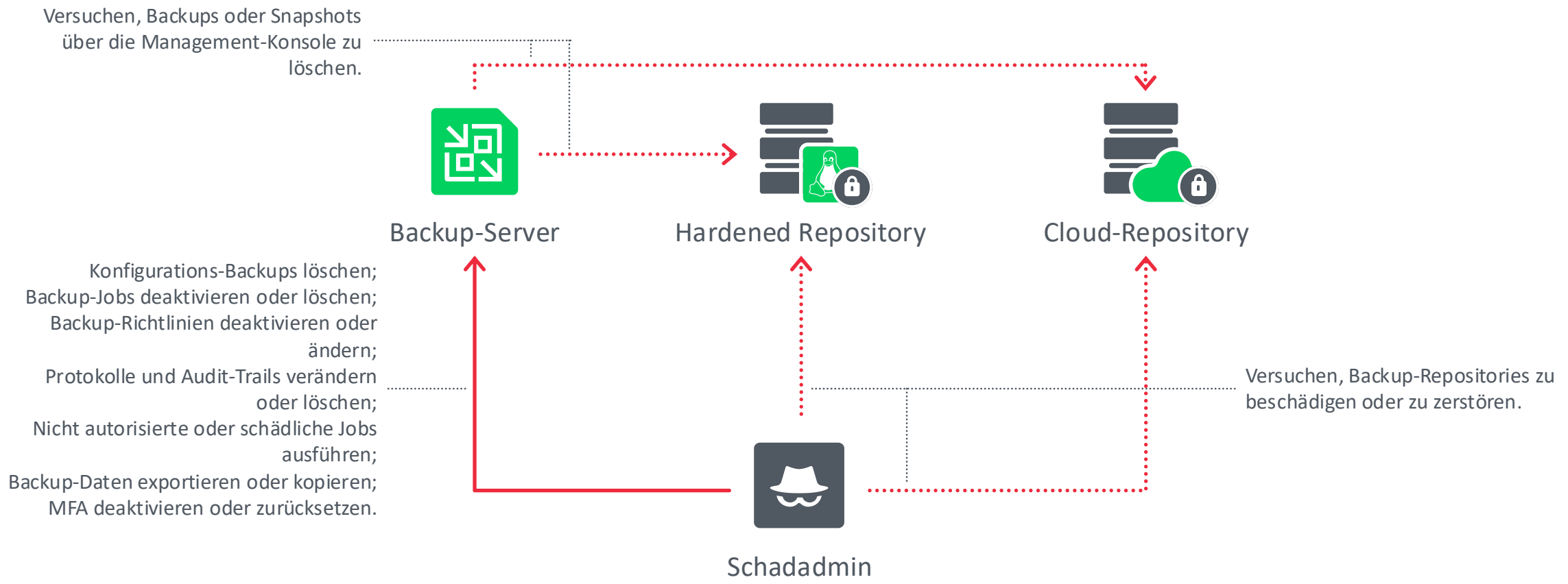
Einige dieser Tools sind Open Source und von der Community erstellt, andere stammen von bekannten Sicherheitsunternehmen. Auch hier gilt: Google bzw. KI hilft weiter.

Risiko #4

Insider-Bedrohungen

Statistik: Authentifizierungsbasierte Angriffe und Insider-Bedrohungen nehmen zu, da privilegierte Benutzer über erweiterten Zugriff auf die kritische Backup-Infrastruktur verfügen.

Insider-Bedrohungen

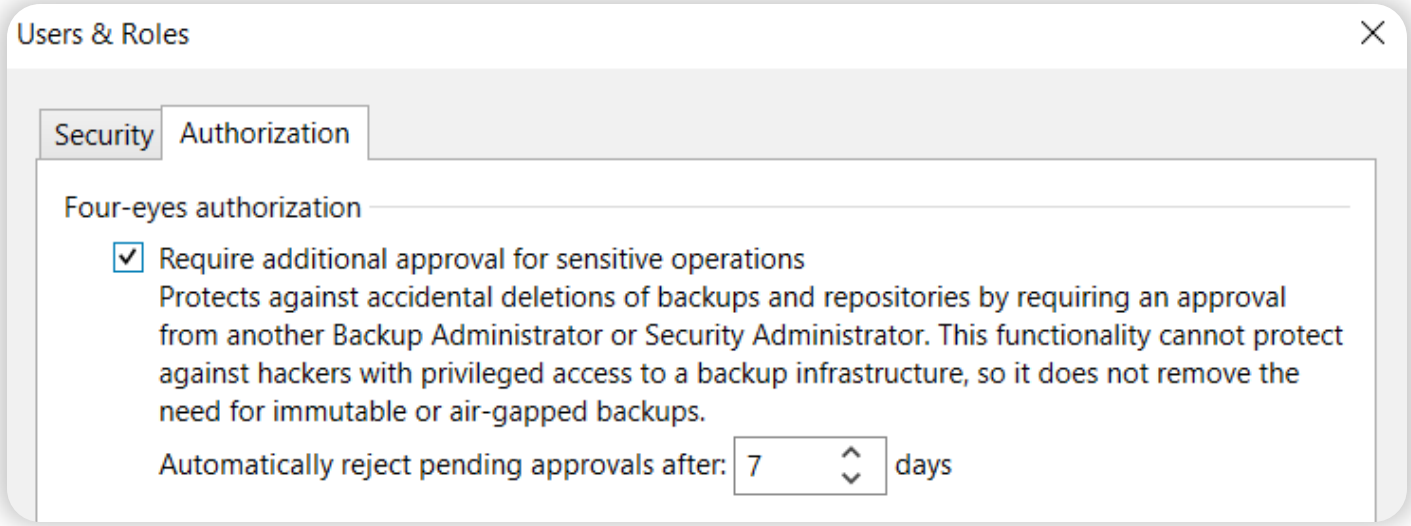


Insider-Bedrohungen

Vier-Augen-Autorisierung

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

- Löschen von Backups, Snapshots oder der Konfigurationsdatenbank
- Ändern oder Entfernen von Backup-Repositories und Speicher
- Verwalten von Benutzer*innen, Gruppen und MFA-Einstellungen
- Aktivieren oder Anpassen automatischer Abmelderichtlinien

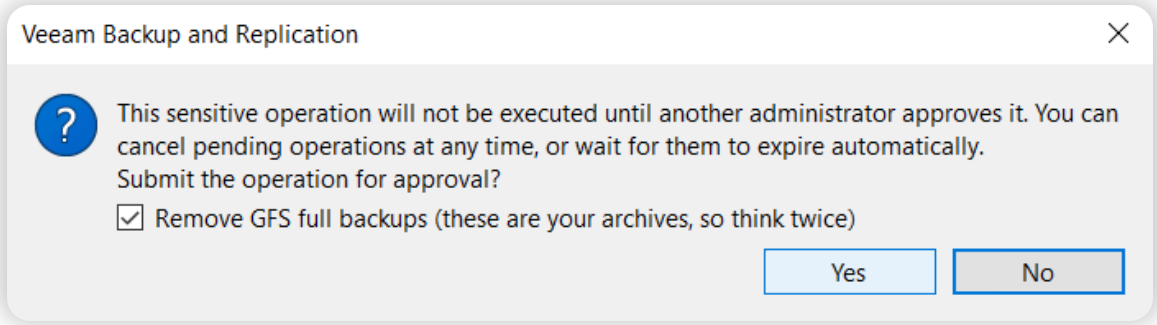


Insider-Bedrohungen

Vier-Augen-Autorisierung

Veeam Backup & Replication unterstützt die Vier-Augen-Autorisierung:

- Wenn ein Admin versucht, Backupdateien zu löschen oder ein Repository zu entfernen, erscheint eine Genehmigungsanfrage unter Pending Approvals.
- Die festgelegten Empfänger*innen erhalten außerdem eine E-Mail-Benachrichtigung.



Insider-Bedrohungen

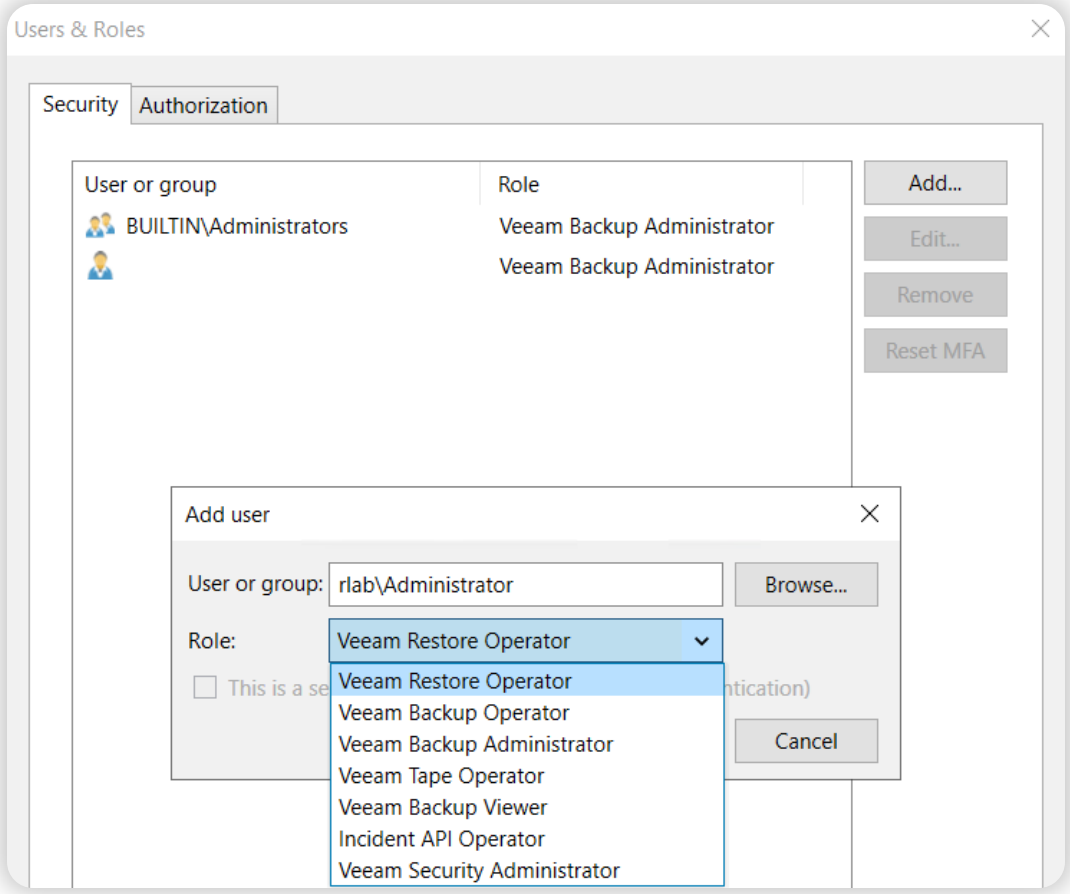
Minimale erforderliche Berechtigungen verwenden

Rollen mit den minimal erforderlichen Berechtigungen zur Ausführung der Aufgabe verwenden.

Reduziert das Risiko unbefugten Zugriffs und von Datenverletzungen.

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

Erhöht die allgemeine Systemsicherheit und Stabilität.



Insider-Bedrohungen

Security Officer

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

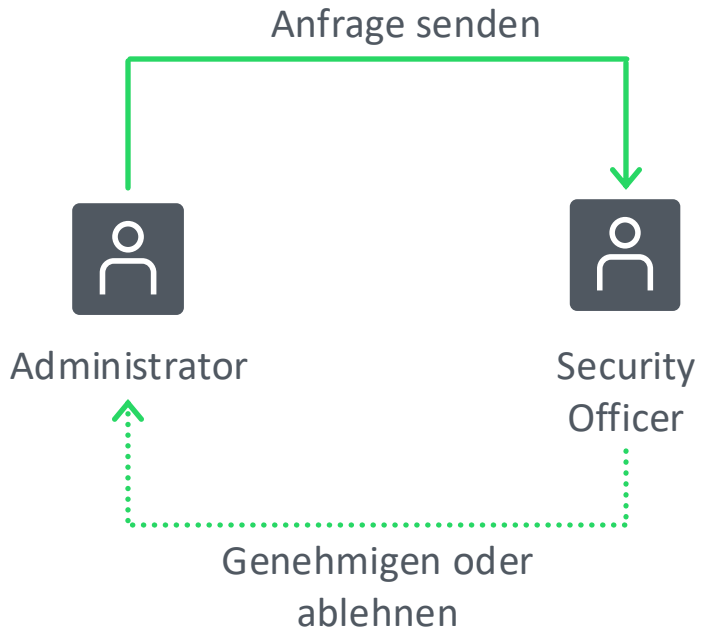
Root-Zugriff für Administratoren und Zurücksetzen von Passwörtern.

Wiederherstellung des Konfigurations-Backups

Aktiviert erweiterte Bereitstellungsoptionen:

- Hochverfügbarkeit
- Lockdown-Modus
- Agent-Bereitstellung für Datenerfassung

Änderung der MFA-Einstellungen



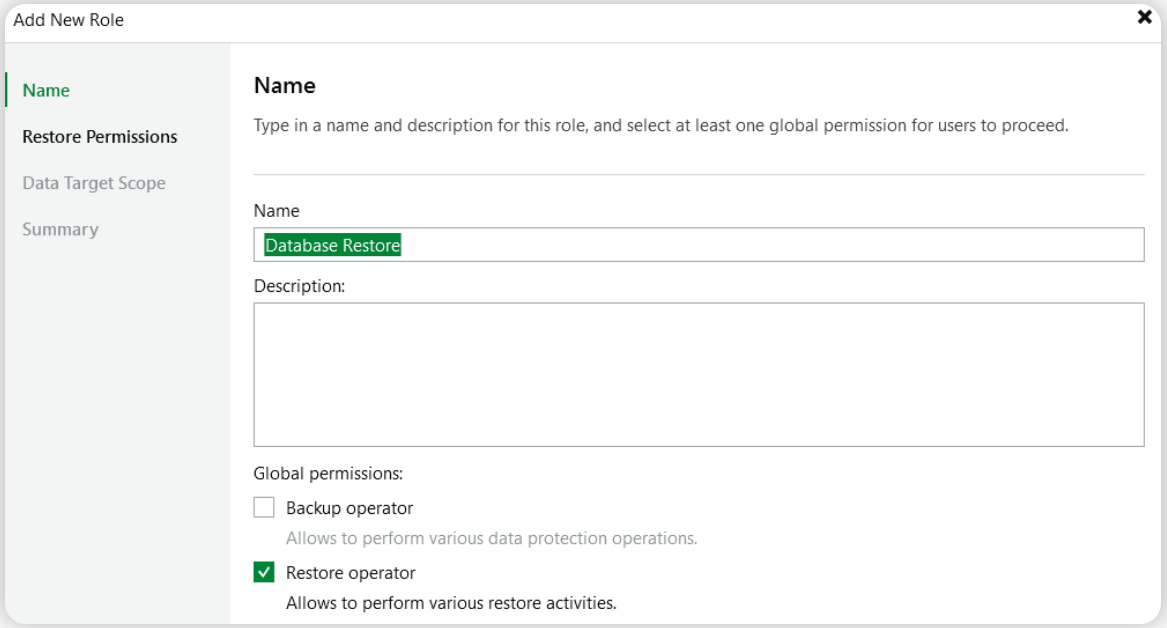
Insider-Bedrohungen

Erweiterte rollenbasierte Zugriffskontrolle

Erweiterte rollenbasierte Zugriffskontrolle ermöglicht es, Benutzerzugriff ausschließlich auf bestimmte Bereiche innerhalb der Backup-Infrastruktur und der Produktionsumgebung zu gewähren.

Es können benutzerdefinierte Rollen erstellt werden, um den Zugriff auf Folgendes zu steuern:

- Backup- und/oder Restore-Vorgänge
- Repository
- Wiederherstellungsoptionen
- Infrastruktur-Objekte

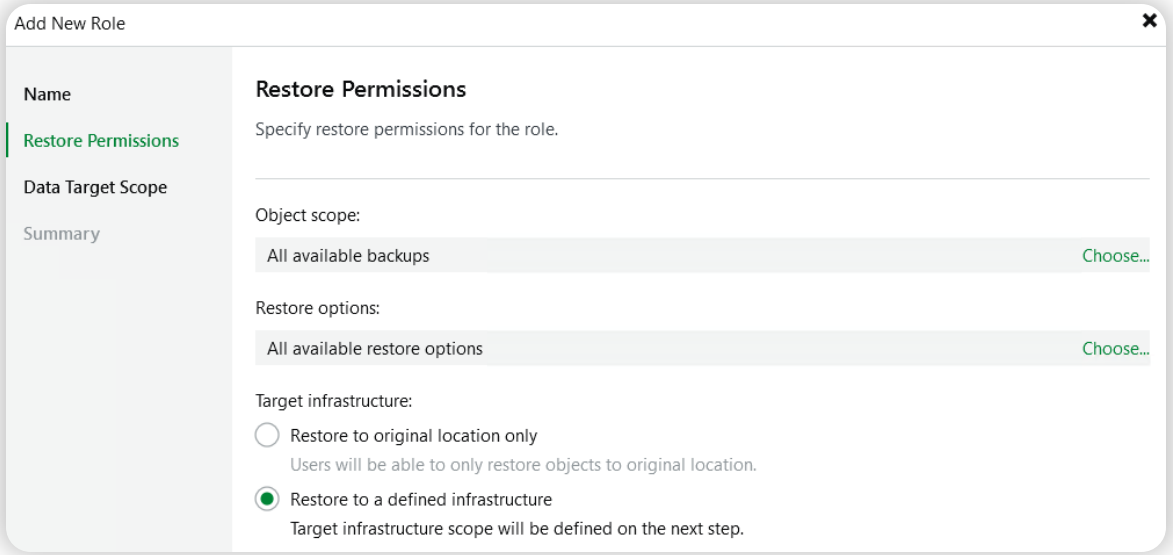


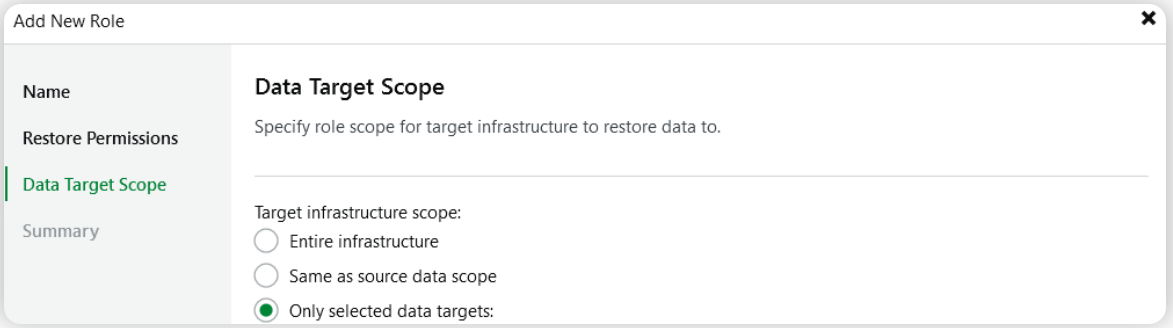
Insider-Bedrohungen

Erweiterte rollenbasierte Zugriffskontrolle

Diese präzise Berechtigungssteuerung ermöglicht es Benutzer*innen, Aufgaben wie Backup oder Wiederherstellung durchzuführen, ohne unnötigen Zugriff auf andere Teile der Infrastruktur zu haben. Dadurch wird die Sicherheit erhöht und das Risiko unbefugter Aktionen reduziert.

Folgen Sie einfach dem Prinzip, nur die minimal notwendigen Zugriffsrechte
zu vergeben.





Insider-Bedrohungen

Überwachung: Veeam ONE für Audits

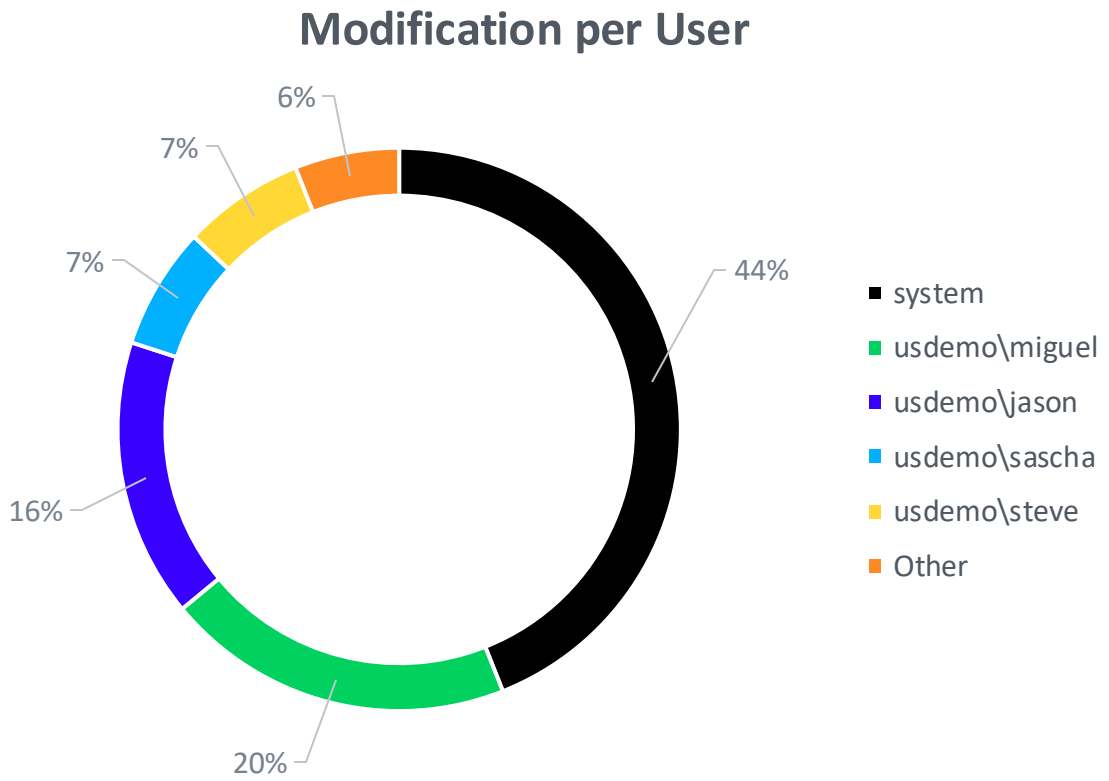
Audit-Informationen zu allen Arten von Wiederherstellungen für Nachvollziehbarkeit.

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

Verfolgt Konfigurationsänderungen in virtuellen Umgebungen mit Benutzerdetails.

Überwacht Zugriffs- und Berechtigungsänderungen zur Sicherstellung der Compliance.

Erstellt umfassende Audit-Berichte für regulatorische und operative Transparenz.



Insider-Bedrohungen

Haben Sie ein unveränderbares Backup?

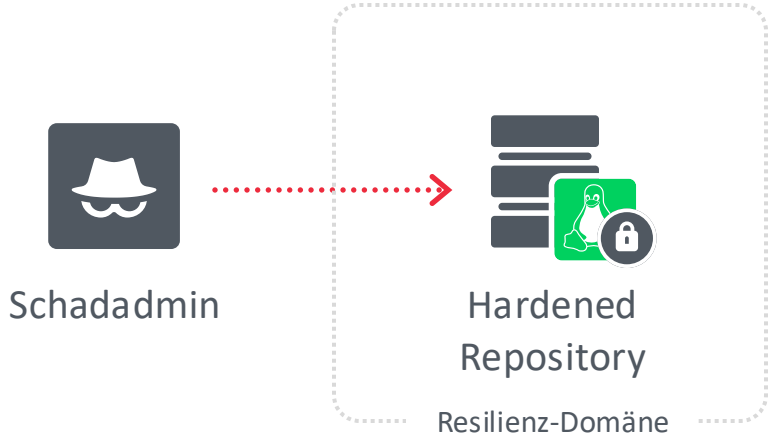
Einmalige Linux-Anmeldedaten, nicht in der Veeam-Datenbank gespeichert

Veeam-Dienste steuern die Datenverkehrsports (virtuelles Airgap)

SSH ist deaktiviert und für Veeam-Upgrades nicht erforderlich

Verhindert unbefugte Änderungen oder das Löschen von Backups

Begrenzt Insider-Bedrohungen, indem die Möglichkeit zur Veränderung oder Löschung gespeicherter Daten eingeschränkt wird



Risiko #5

Netzwerkbasierte laterale Bewegung

Statistiken: Die mediane Verweildauer beträgt 26 Tage, wenn externe Stellen den Vorfall melden, aber nur 5 Tage in Ransomware-Fällen, in denen die Angreifer selbst die Opfer informieren.

Netzwerkbasierte laterale Bewegung

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

Angreifer stoppen selten bei dem System, das sie zuerst kompromittieren. Stattdessen kartieren sie die Umgebung, greifen weitere Systeme an und passen ihre Taktik an die vorgefundenen Sicherheitsmaßnahmen an.

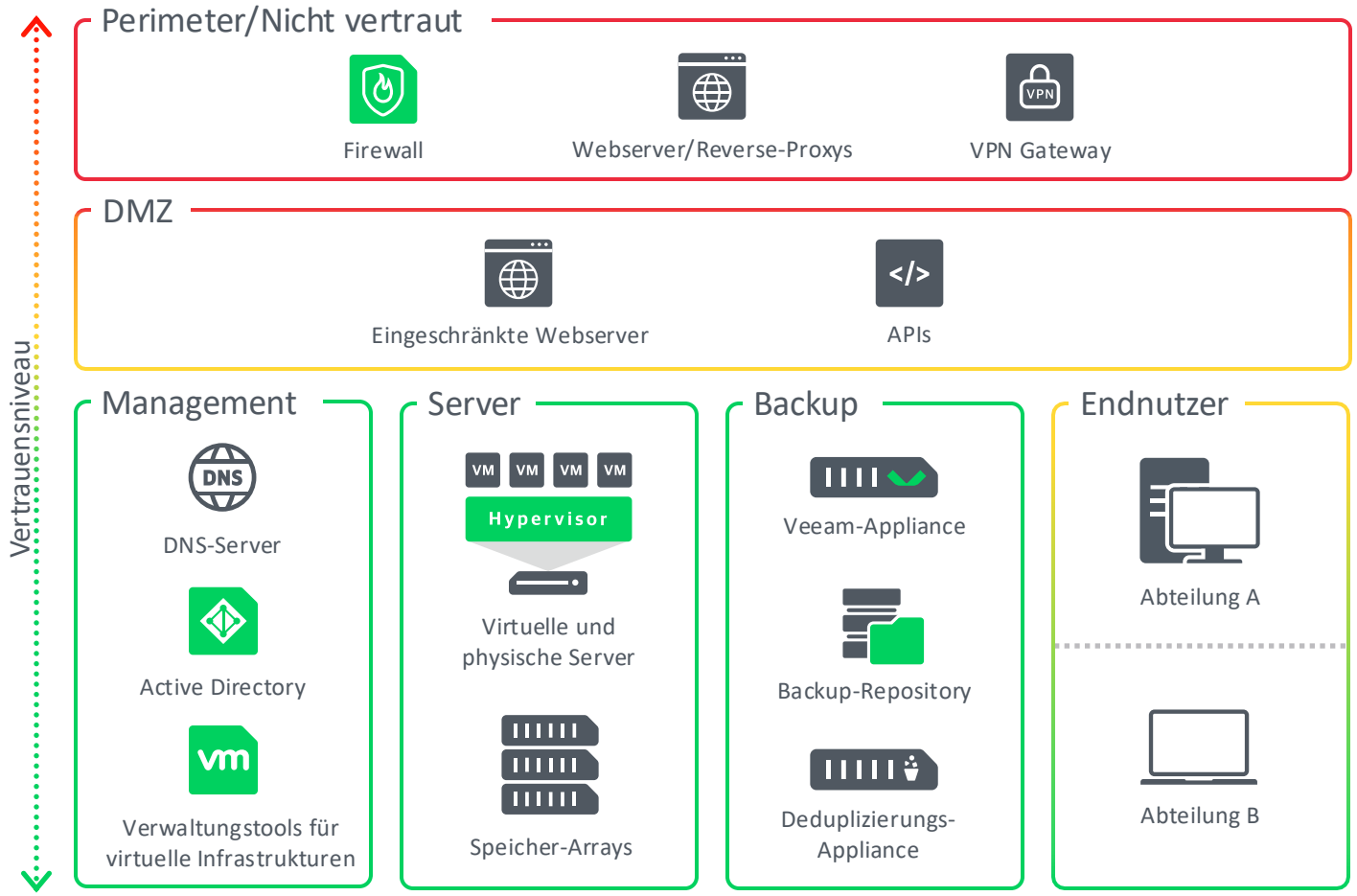
Laterale Bewegung kann legitime Werkzeuge nutzen (PowerShell- und BASH-Skripte, WMI, RDP, SSH, Nmap, SCP, Netzwerkfreigaben usw.), um unauffällig zu bleiben. Das macht die Erkennung besonders schwierig.

Angreifer nutzen Schwächen in der Netzwerksicherheit aus (z. B. mangelnde Segmentierung, weitreichende Berechtigungen, domain-gebundene Backup-Server), um sich seitlich auszubreiten und weitere Systeme zu kompromittieren.

Wie bereits bekannt: Die Backup-Infrastruktur ist ein besonders wertvolles Ziel für laterale Bewegung, da Angreifer die Disaster-Recovery-Fähigkeiten sabotieren wollen.

Netzwerkbasierte laterale Bewegung

Netzwerksegmentierung: Beispiel für Zonen



Begrenzt laterale Bewegung

Es sind nur notwendige Kommunikationswege erlaubt. Angreifer können nicht ohne Weiteres von kompromittierten auf kritische Systeme übergehen.

Harmoniert optimal

Lässt sich mit aktiver Bedrohungserkennung wie XDR/EDR, Honeypots zur Ablenkung von Angreifern und SIEM zur Überwachung kombinieren.

Ermöglicht Compliance

Segmentierte Architekturen unterstützen gesetzliche und regulatorische Anforderungen und schützen die Organisation sowohl betrieblich als auch rechtlich.

Netzwerkbasierte laterale Bewegung

Was gibt es außer Netzwerksegmentierung noch?

Verschlüsselte Kommunikation

Veeam verschlüsselt Verwaltungsverbindungen standardmäßig mit selbstsignierten TLS-Zertifikaten. Es ist jedoch möglich, ein von einer internen Zertifizierungsstelle signiertes Zertifikat zu verwenden, um die Kontrolle zu verbessern.

Härtung der Backup-Infrastruktur

MFA, Key Management System, Four-Eyes, RBAC, kein Beitritt zur AD-Domäne usw.

Monitoring

Veeam B&R/ONE generiert Echtzeitwarnungen zu Backup-Fehlern, Job-Anomalien oder ungewöhnlichen Aktivitätsanstiegen, die auf Ransomware oder eine Kompromittierung der Infrastruktur hinweisen können, und leitet diese Warnungen direkt an ein SIEM weiter.
Das SIEM kann diese Ereignisse mit Sicherheitsanomalien im restlichen Netzwerk abgleichen und damit schneller sichtbar machen, wenn die Backup-Umgebung gefährdet ist.

VBR-Sicherheitsbest Practices: Hardening

Leitfaden zu SIEM (Security Information & Event Management)

Netzwerkbasierte laterale Bewegung

Hör nicht auf, gegen Shadow IT zu kämpfen!

Erweitert die Angriffsflächen

Nicht autorisierte Apps, Cloud-Plattformen oder Remote-Zugriffswerkzeuge schaffen versteckte Pfade, die Angreifer ausnutzen können. Diese Pfade umgehen oft Standard-Netzwerkkontrollen und Monitoring.

Anmeldedaten-Leckage und Bridging

Benutzer könnten Passwörter über nicht genehmigte Kanäle speichern oder teilen (z. B. E-Mail, Chat-Apps oder persönliche Dateispeicher). Dadurch erhalten Angreifer Einstiegspunkte für laterale Bewegung auf Basis kompromittierter Zugangsdaten.

Erleichtert unauffällige laterale Bewegung

Angreifer können Shadow-IT-Tools zum Ablegen von Daten, Ausführen von Befehlen oder Übertragen von Malware nutzen – und sich damit in normalen Datenverkehr einfügen, was die Erkennung durch herkömmliche Methoden erheblich erschwert.

Reduziert Monitoring und verwertbare Erkenntnisse

Traditionelle SIEMs und Backup-Monitoring haben es deutlich schwerer, laterale Bewegung zu erkennen, wenn Shadow IT genutzt wird, da Logs und Datenverkehr möglicherweise nicht über genehmigte oder überwachte Kanäle laufen.

Risiko #6

Datenvergiftung

Statistik: Datenvergiftungsangriffe stellen eine besonders ausgefeilte Bedrohung dar, bei der Cyberkriminelle Daten unbemerkt vor dem Backup-Vorgang manipulieren. Dadurch werden Backups unzuverlässig und im Ernstfall nicht mehr für Wiederherstellungen geeignet.

Datenvergiftung

Was ist Datenvergiftung?

Datenvergiftung in Backups bezeichnet einen ausgefeilten Cyberangriff, bei dem Angreifer die Originaldaten unauffällig verändern oder beschädigen, bevor sie gesichert werden. Diese schädlichen Modifikationen bleiben oft über lange Zeiträume unbemerkt und machen Backup-Kopien unzuverlässig oder kompromittiert, was die gesamte Wiederherstellungsstrategie untergräbt.

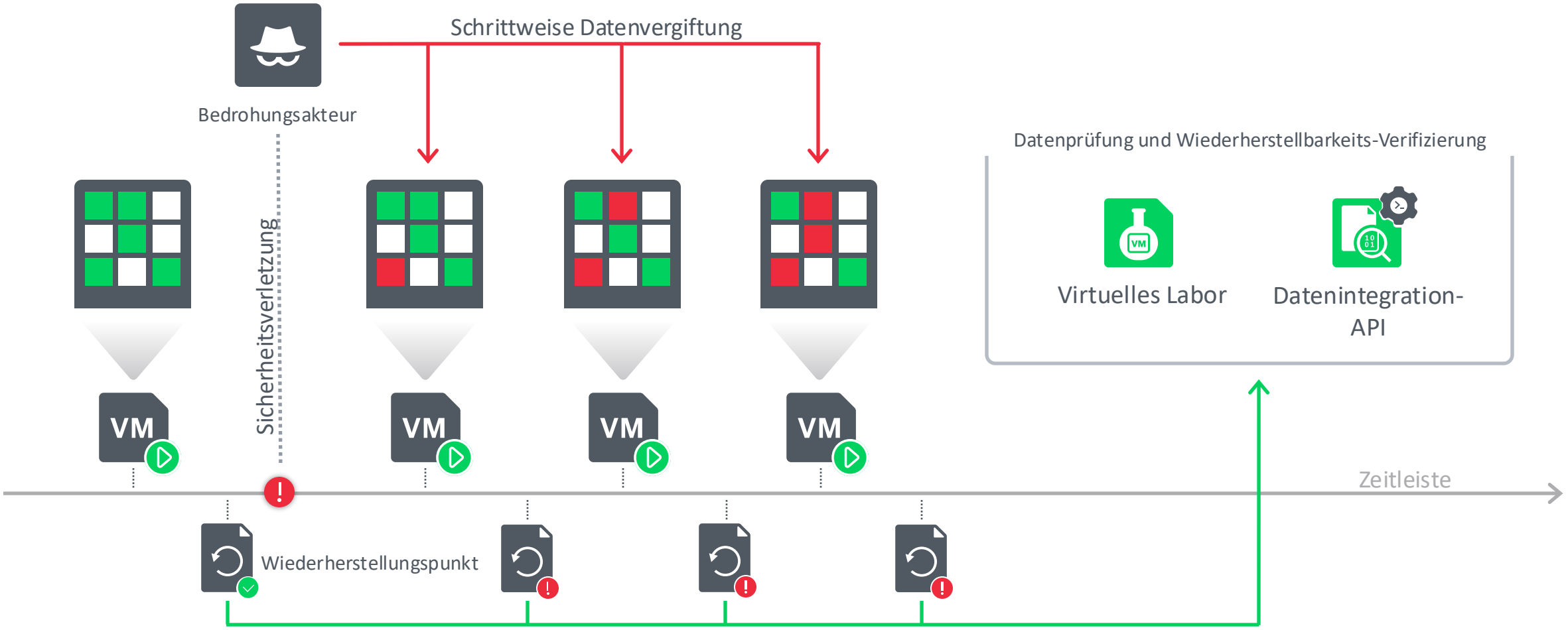
Die Änderungen erfolgen so, dass sie wie normale Fehler oder Routineaktualisierungen wirken. Über Wochen, Monate oder sogar Jahre summieren sich diese kleinen Veränderungen. Schließlich sind die Daten so verfälscht, dass sie Probleme verursachen – etwa finanzielle Verluste, falsche Statistiken oder Fehler in Berichten und Entscheidungen.

Im Gegensatz zu traditioneller Ransomware oder zerstörerischen Angriffen zielt Datenvergiftung direkt auf die Gültigkeit und Integrität der Daten ab, sodass selbst wiederhergestellte Dateien korrumpiert sind oder ungültige/veränderte Inhalte aufweisen.

Solche Angriffe bleiben oft unentdeckt, bis Daten validiert oder Wiederherstellungen versucht werden, was zu teuren Ausfallzeiten und Datenverlust führt.

Datenvergiftung

Schrittweise oder „Low and Slow“



Datenvergiftung

Virtuelles Labor und Datenintegration-API

Clean-Room-Datenwiederherstellung: Verbesserung von Sicherheit und Datenintegrität

Das virtuelle Labor ist eine „Clean Room“- oder „Sandbox“-Umgebung, die es SureBackup-Jobs ermöglicht, Ihre Backups zu testen, ohne Produktionssysteme zu beeinträchtigen. Diese Umgebung erlaubt es Ihnen, Backups wiederholt auf *Wiederherstellbarkeit* und *Inhaltsintegrität* zu prüfen.

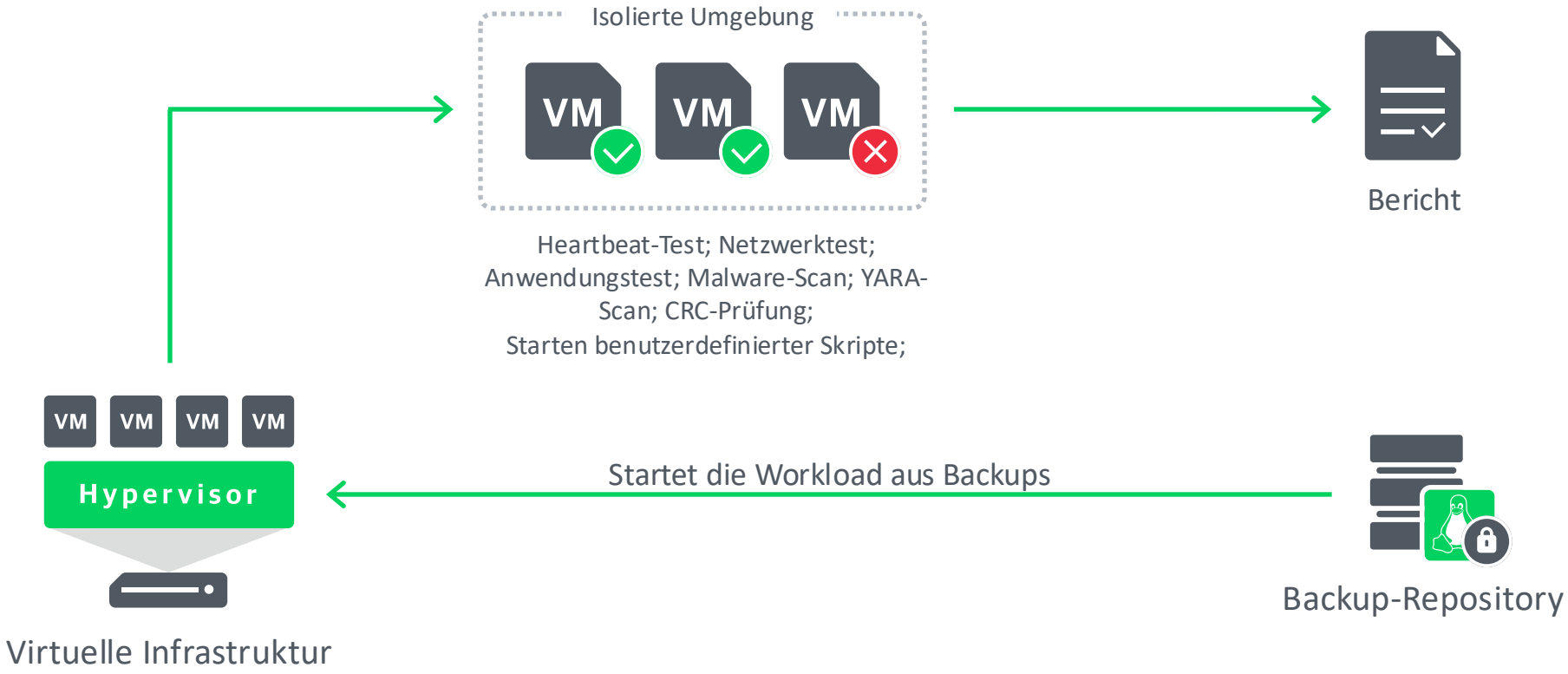
SureBackup verifiziert, dass kritische Dienste – wie Datenbanken, Active Directory oder E-Mail-Systeme – innerhalb der Sandbox korrekt funktionieren. Ungewöhnliches Anwendungsverhalten während dieser Tests kann auf versteckte Formen von Datenvergiftung hinweisen.

Die Datenintegration-API ermöglicht das Einbinden von Backup-Daten, ohne sie vollständig wiederherzustellen. Dadurch können Sie Skripte, Data Mining, Klassifizierung, Analysen oder forensische Tools automatisiert auf die Backup-Daten anwenden.

Sie können aktuelle Backups mit vertrauenswürdigen, sauberen Backups vergleichen, um Datenabweichungen oder unautorisierte Änderungen zu erkennen. Verdächtige oder veränderte Datensätze können für detaillierte manuelle Analysen oder Massenberichte exportiert werden.

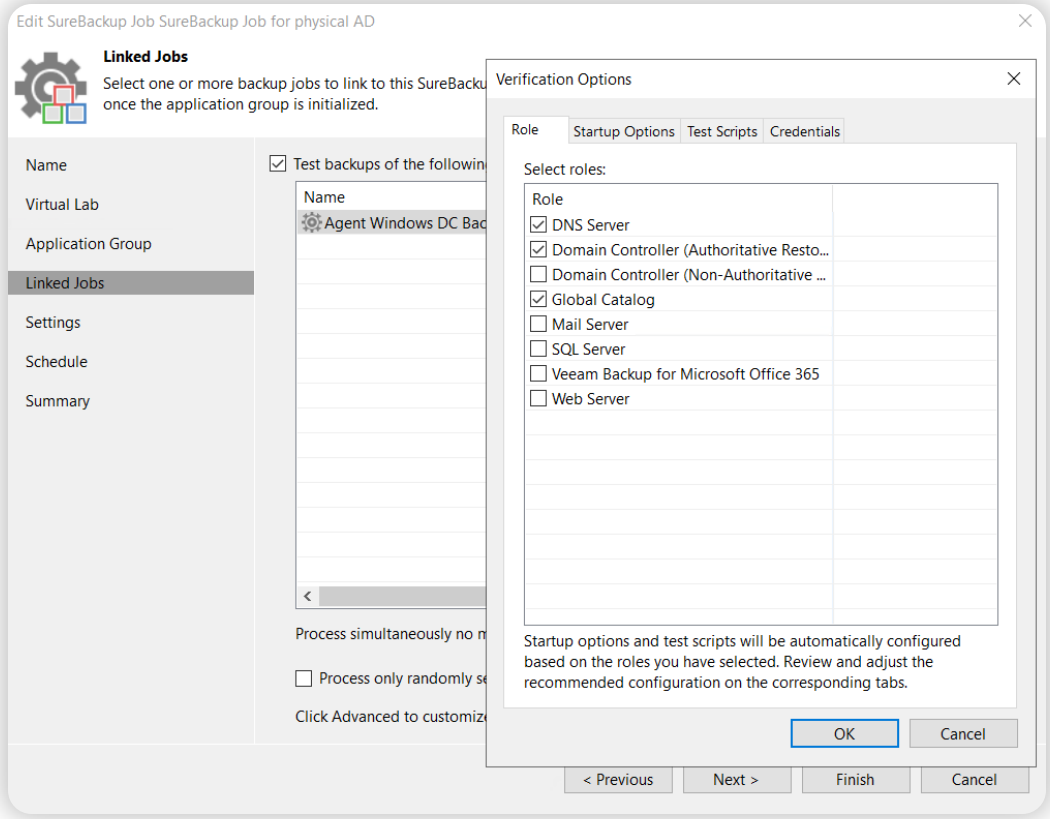
Datenvergiftung

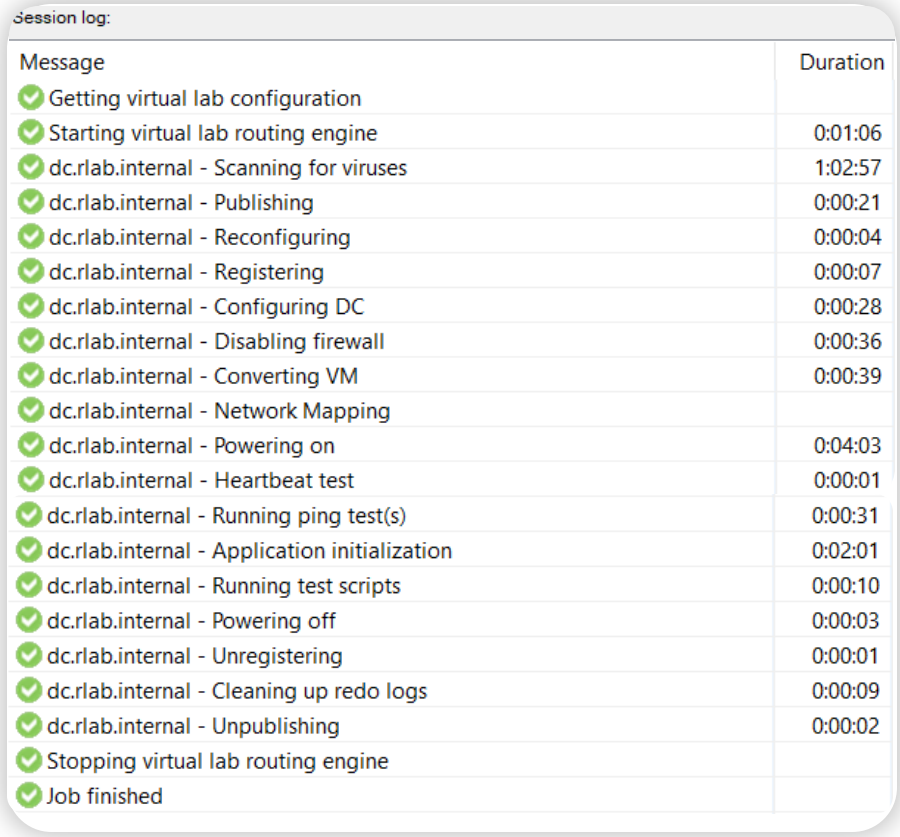
SureBackup-Workflow



Datenvergiftung

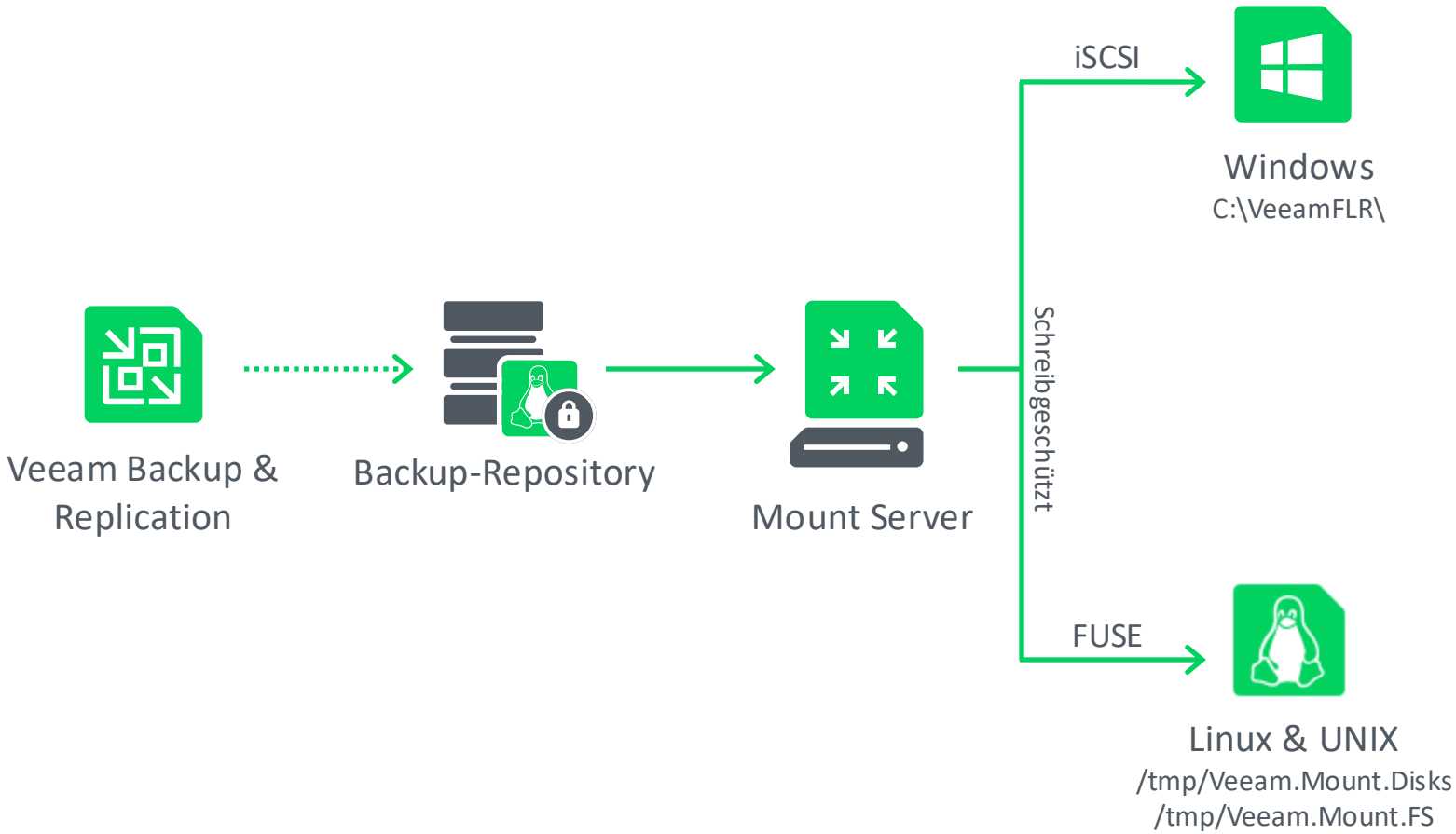
SureBackup





Datenvergiftung

Workflow der Datenintegration-API



Anwendungsfälle

- Datenauswertung
- Klassifizierung
- Analytik
- Forensische Tools
- Sicherheitsanalyse
- Malware-Scan
- eDiscovery
- DSGVO-Auditierung
- ML-Anwendungen
- Datenvergleich
- Integritätsprüfung

Datenvergiftung

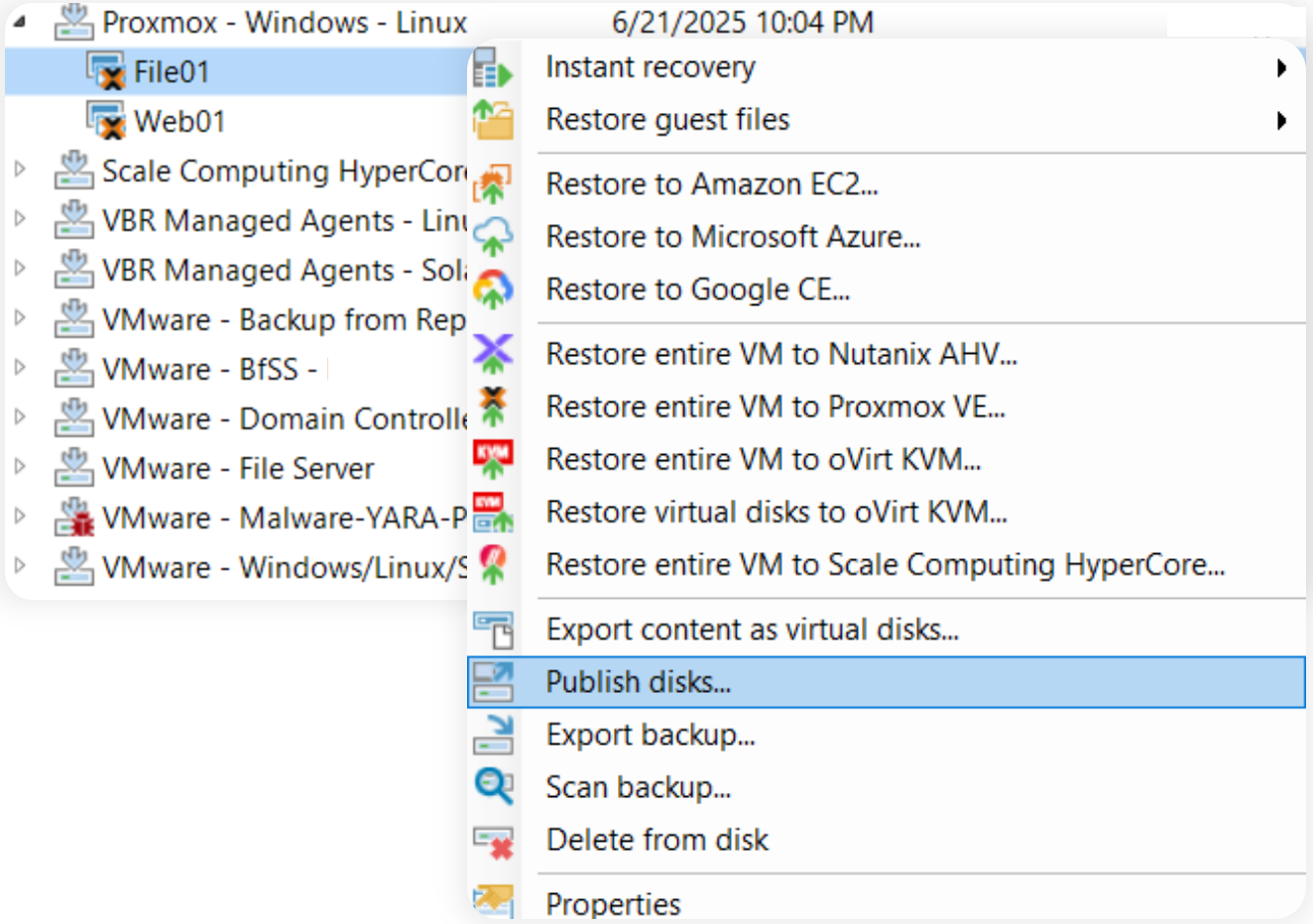
Datenintegration-API

Die Datenintegration-API (REST) ist die programmgesteuerte Version von „Datenträger veröffentlichen…“.

Sie ermöglicht Automatisierung, Integration und wiederholbare Workflows.

Im Grunde genommen ist es das „Backend“, das von „Datenträger veröffentlichen…“ im Hintergrund verwendet wird.

Es ist auch möglich, PowerShell-Skripte zu nutzen, um „Datenträger veröffentlichen…“ zu automatisieren.



Risiko #7

Allgemeine Umgebungsschwachstellen

Viele Organisationen verfügen nicht über korrekt umgesetzte Sicherheitskonfigurationen – selbst dann, wenn Playbooks und Best Practices vorhanden sind.

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

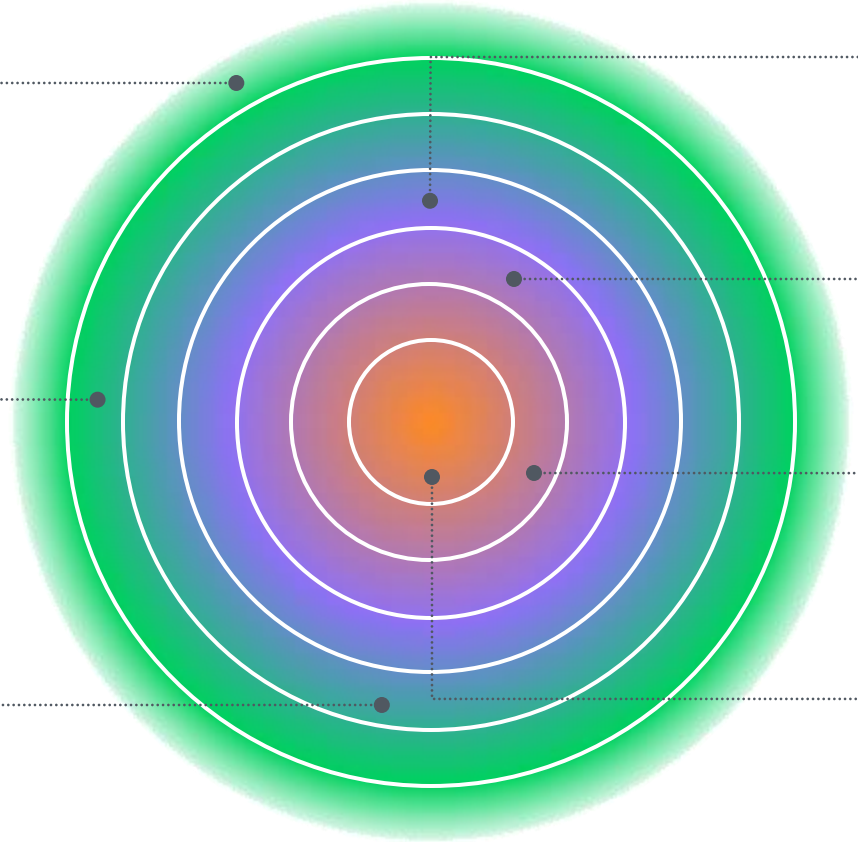
Allgemeine Umgebungsschwachstellen

Sicherheitsebenen

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

Perimetersicherheit
Dies ist der „äußere Zaun“, an dem externe Angreifer abgewehrt oder blockiert werden.

Netzwerksicherheit
Verhindert laterale Bewegung und begrenzt die Ausbreitung von Bedrohungen innerhalb der Umgebung.



Endpunktsicherheit
Jedes Gerät (PC, Server, Mobilgerät) ist ein potenzieller Einstiegspunkt.

Applikationssicherheit
Anwendungen sind häufige Ziele für Angriffe und Ausnutzung.

Datensicherheit
Das eigentliche Ziel sind die Daten – ob Diebstahl, Erpressung oder Sabotage.

Kritische Geschäftsressourcen
Systeme/Daten, die für die Geschäftskontinuität essenziell sind, benötigen besondere Schutzmaßnahmen.

Allgemeine Umgebungsschwachstellen

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?

Allgemeine Umgebungsschwachstellen

It's not just about VDP configuration

Denken Sie allgemein über Ihre Umgebung nach…

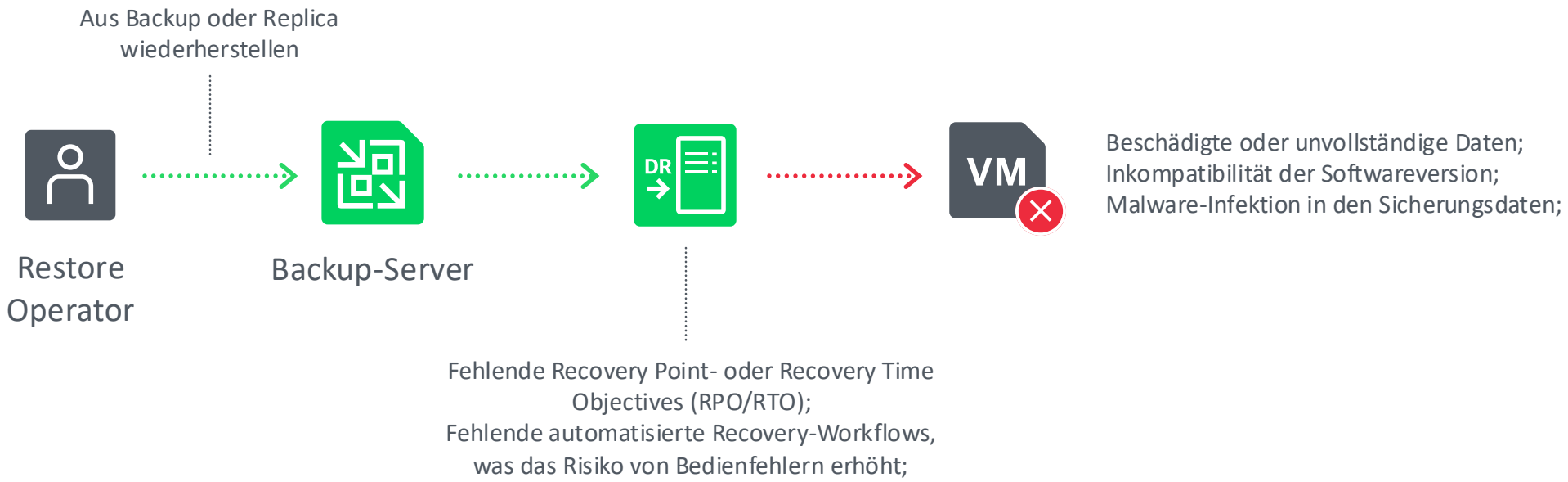
1. Wann haben Sie zuletzt die Liste der Administratoren auf inaktive/„Geist“-Konten überprüft?
2. Wie viele aktive Firewall-Regeln erlauben mehr als nötig? Suchen Sie einfach nach „allow any“.
3. Haben Sie schon einmal einen Portscanner aus nicht vertrauenswürdigen bzw. halb vertrauenswürdigen Netzwerken 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)…

Risiko #8

Wiederherstellungs- und Orchestrierungsfehler

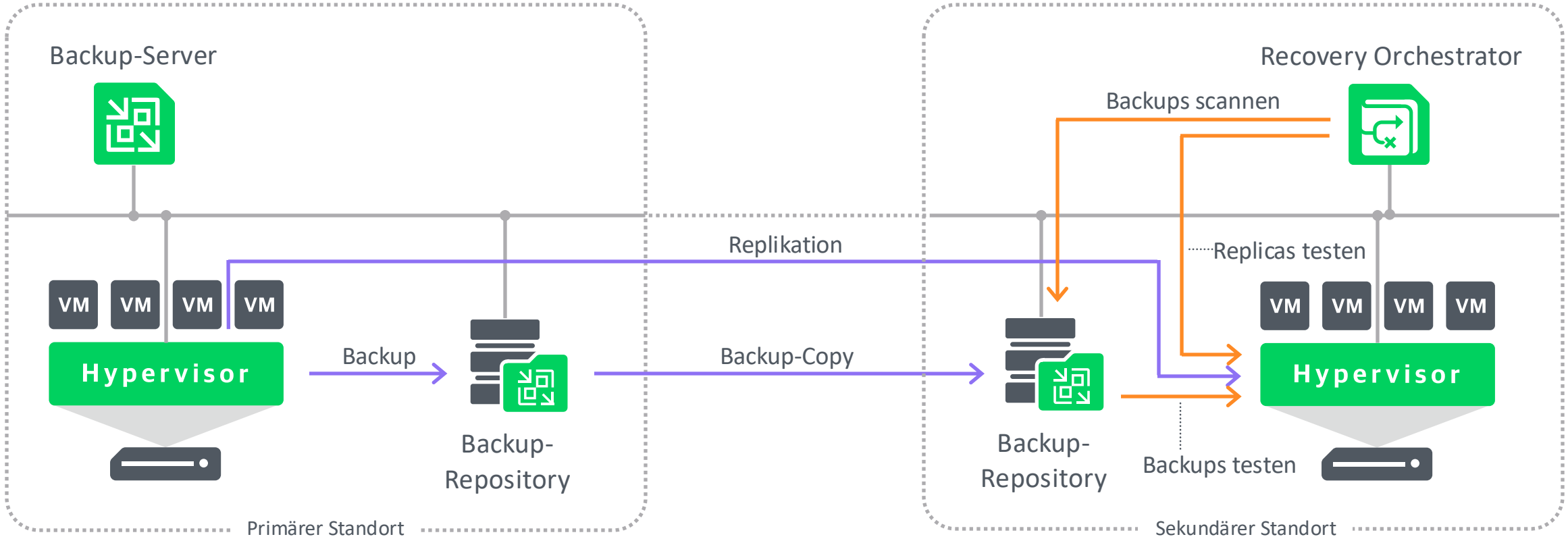
Fehler bei der Disaster Recovery und der Recovery-Orchestrierung werden häufig durch unzureichende Tests, veraltete Wiederherstellungspläne sowie fehlende Dokumentation oder Automatisierung verursacht.

Wiederherstellungs- und Orchestrierungsfehler



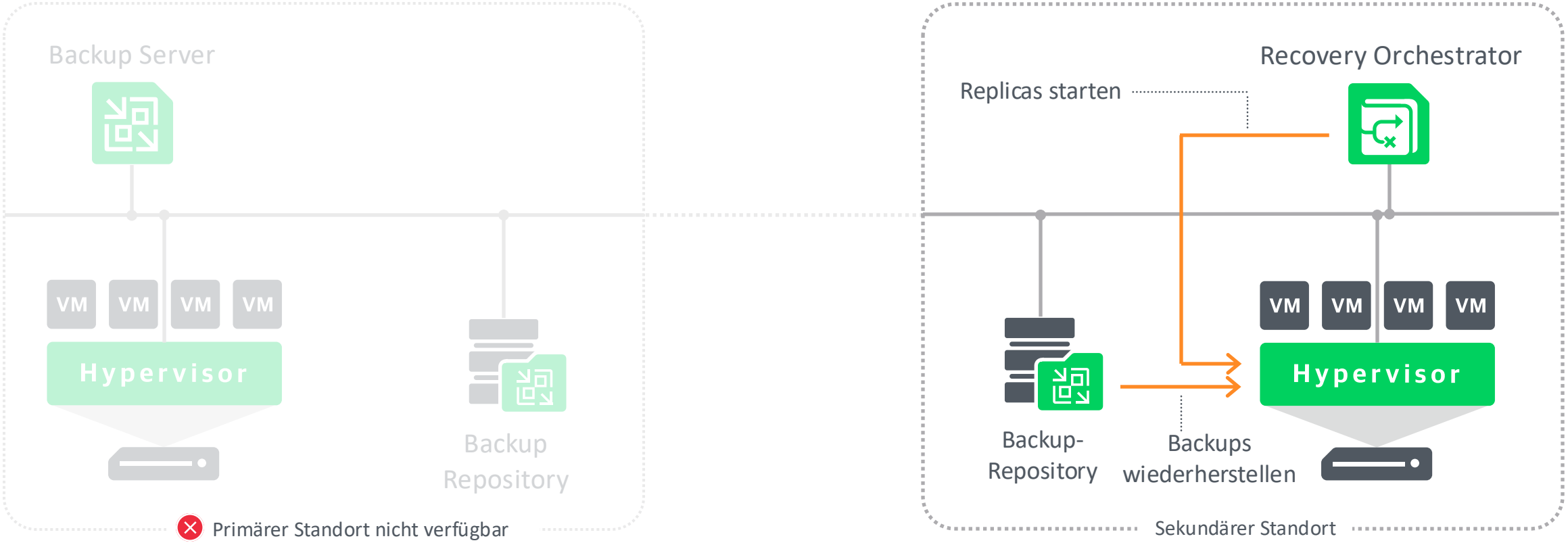
Wiederherstellungs- und Orchestrierungsfehler

Regulärer Betrieb



Wiederherstellungs- und Orchestrierungsfehler

Failover



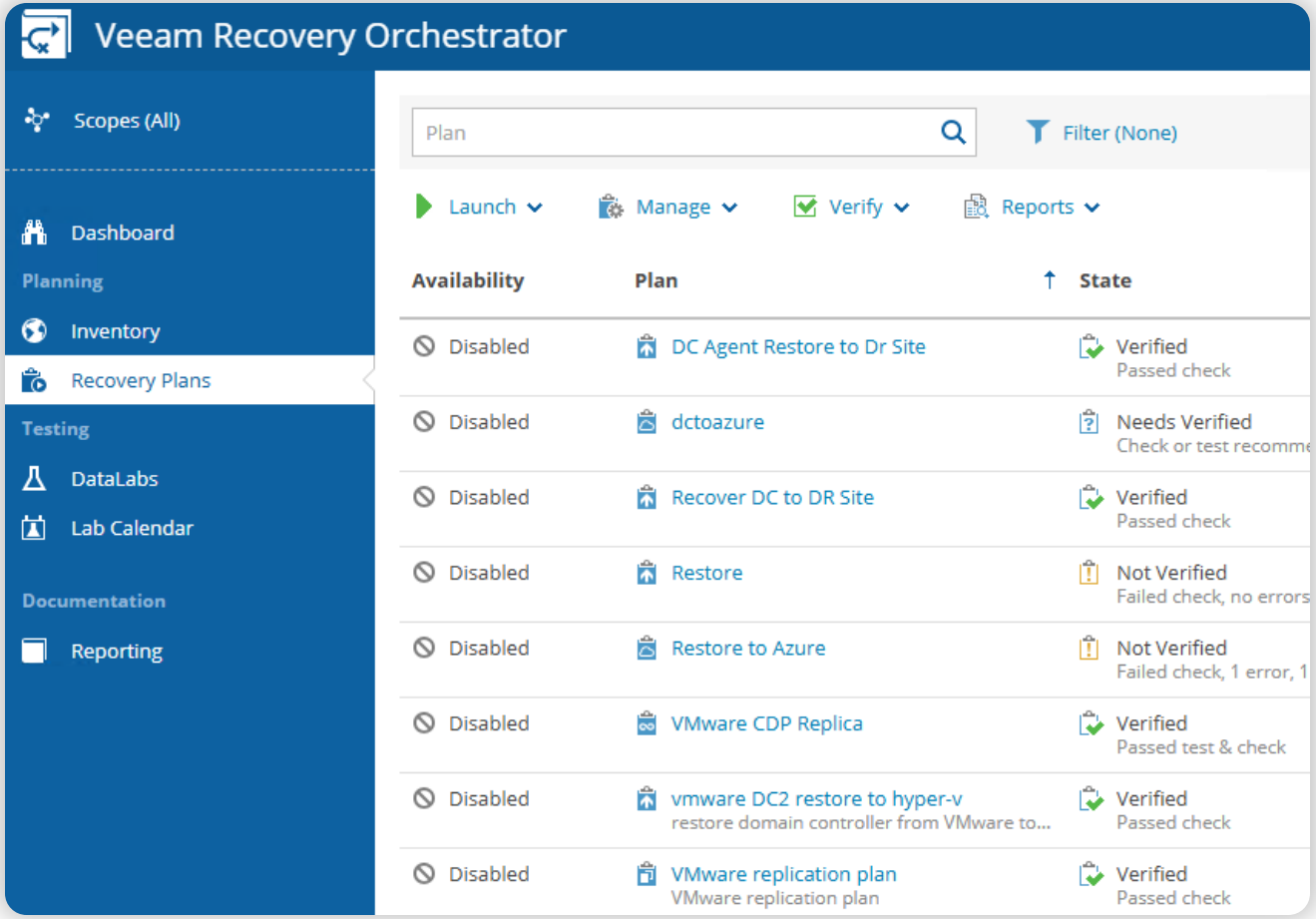
Wiederherstellungs- und Orchestrierungsfehler

Plan erstellen

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

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

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



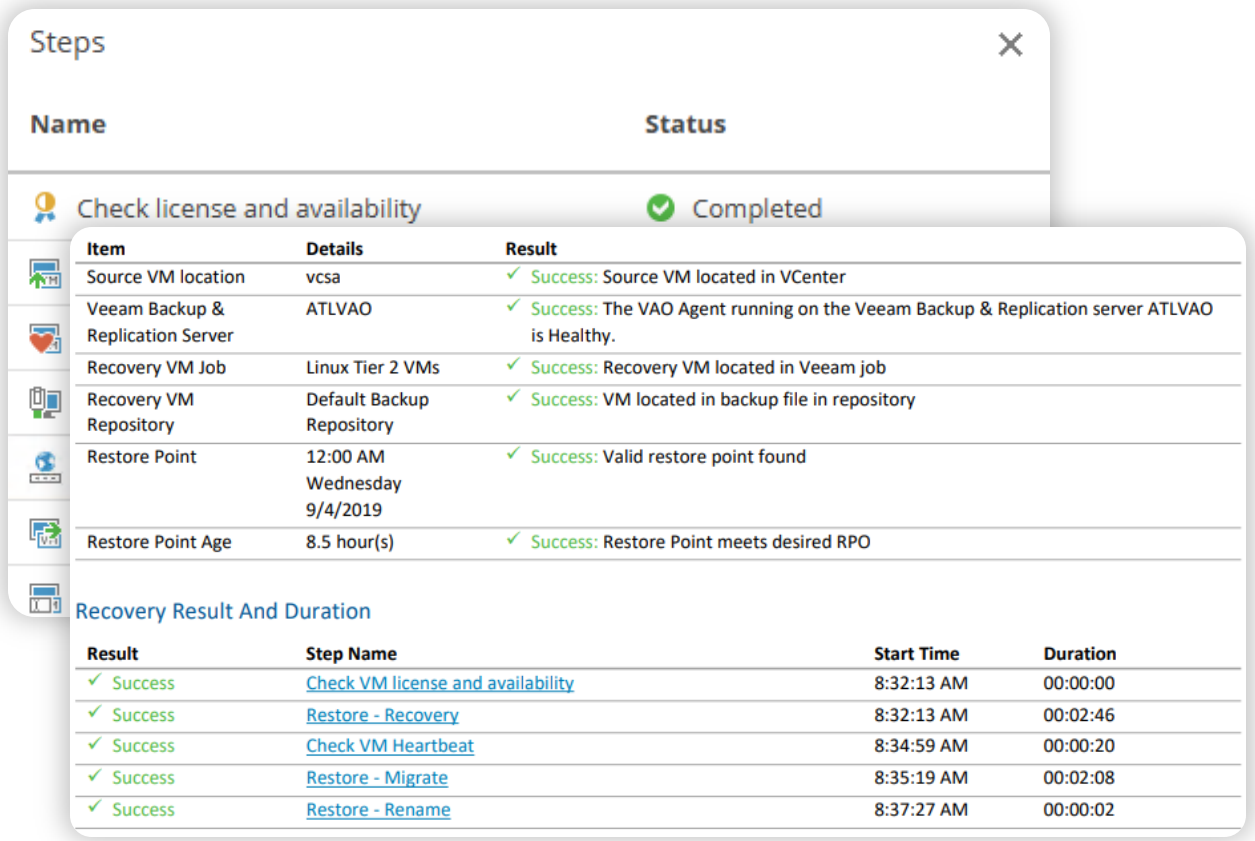
Wiederherstellungs- und Orchestrierungsfehler

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.



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

Follow us!

Join the community hub: