Veeam Data Platform

Security Best Practices

Pavel Kosarev

Manager, Systems Engineers

Nikita Kozlenko

Manager, Systems Engineers

Agenda

1 Protecting the Data Protection Environment

2 Safeguarding Backups from Loss or Ransomware

3 Preventing Reinfection

4 Limiting Internal Risks

5 Reducing the Risk of Widespread Breach

6 Tracing Corrupted or Manipulated Data

7 Extending Security Beyond Backup Solutions

8 Enabling Confident, Fast Disaster Recovery

Note about the materials and resources

This slide deck includes many clickable links to various articles and other resources for your further learning and exploration.

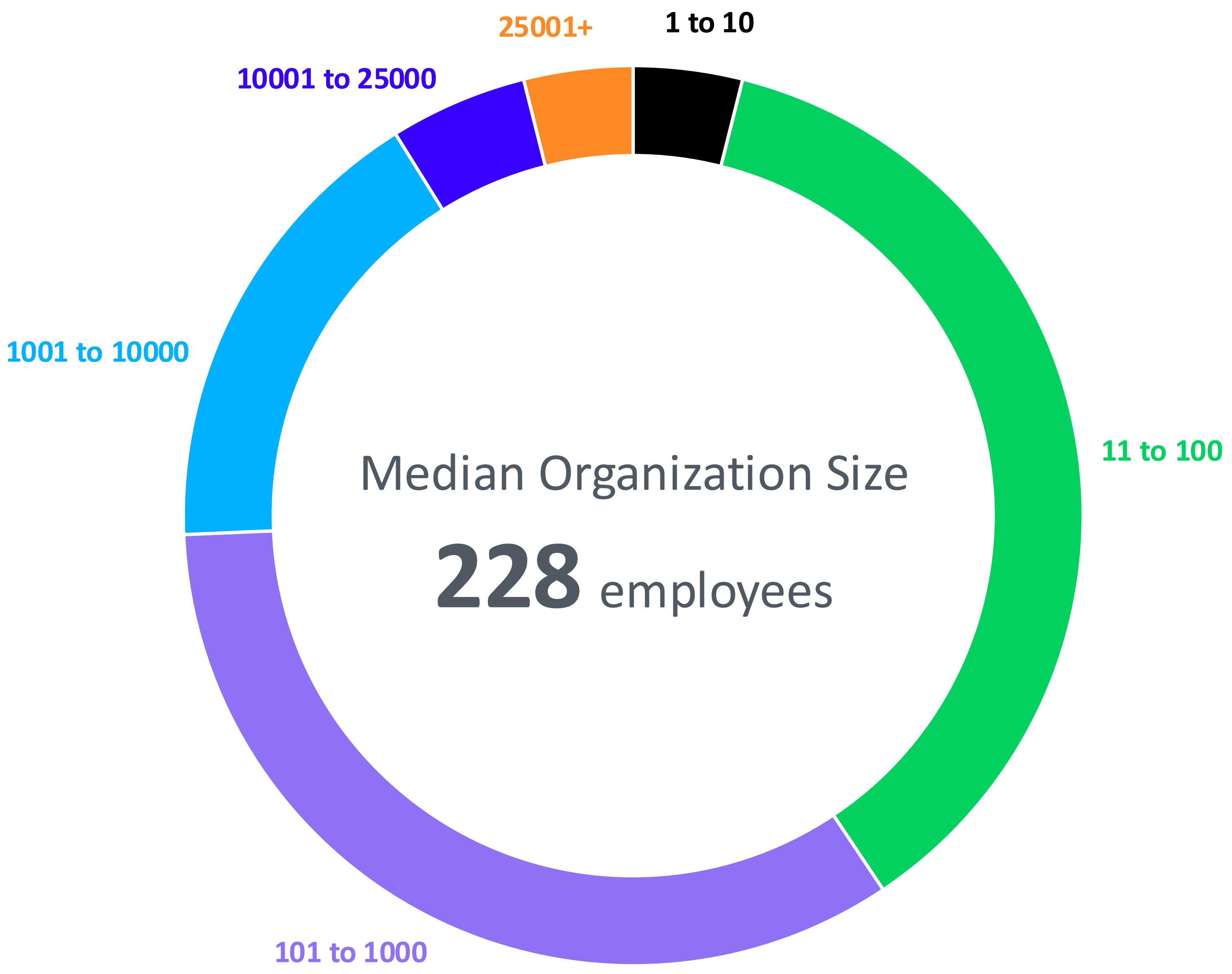
A PDF version of this slide deck will be provided to you via email shortly after the completion of this training session. Please keep an eye on your inbox.

The illusion of safety

69% of ransomware victims believed they were prepared before the breach – but reported a 20% drop in that confidence post-incident.

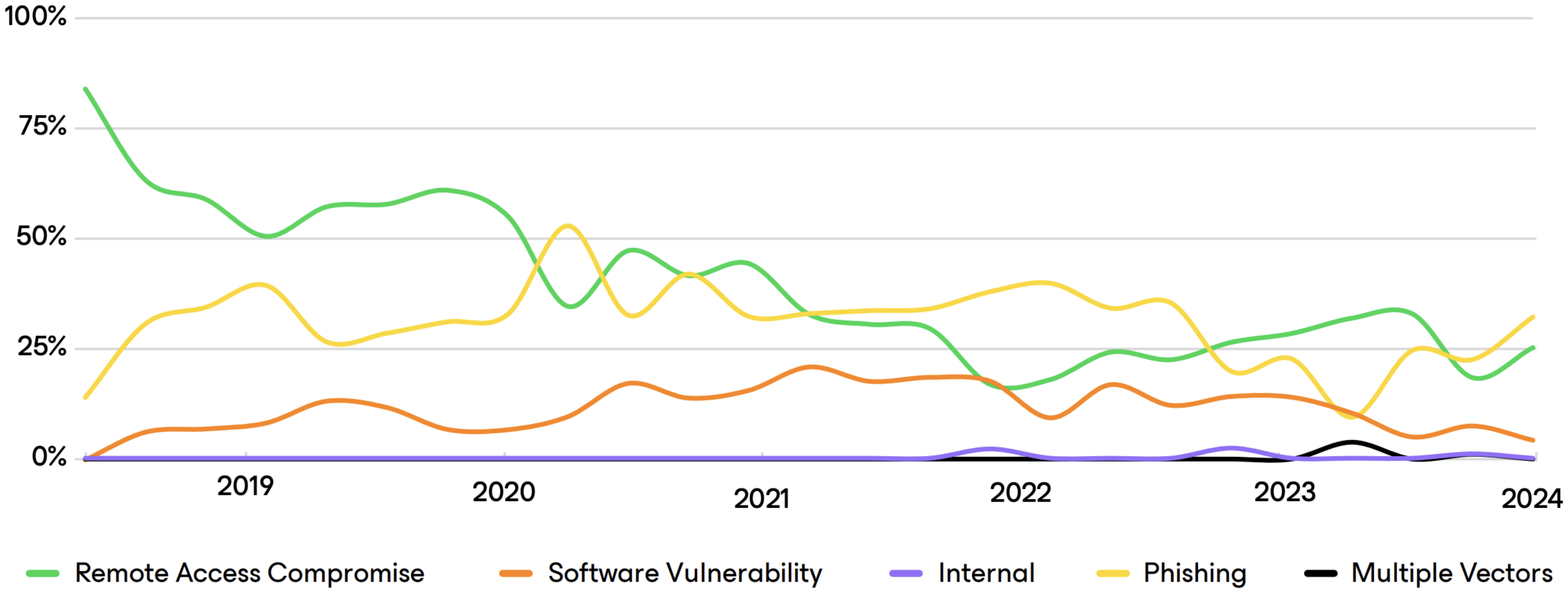
Attacks can hit organizations of any size.

Ransomware Impacted Organizations by Employee Count in Q1 of 2025



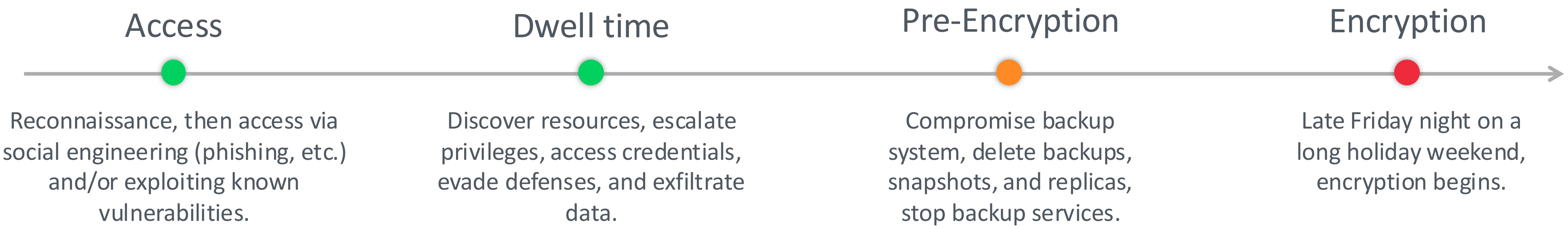
Source: https://www.coveware.com/blog/2025/4/29/the-organizational-structure-of-ransomware-threat-actor-groups-is-evolving-before-our-eyes

How are attackers gaining access?



Source: 2025 Ransomware Trends and Proactive Strategies by Veeam

Simplified Timeline for Cyber Attacks



Access

Reconnaissance, then access via social engineering (phishing, etc.) and/or exploiting known vulnerabilities.

Dwell time

Discover resources, escalate privileges, access credentials, evade defenses, and exfiltrate data.

Pre-Encryption

Compromise backup system, delete backups, snapshots, and replicas, stop backup services.

Encryption

Late Friday night on a long holiday weekend, encryption begins.

What threats do you need to guard against?

Infrastructure Security

- Backup Server Compromise
- Network-Based Lateral Movement
- General Environment Vulnerabilities

Data Security

- Backup Data Encryption/Deletion
- Malware in Backups
- Data Poisoning in Backup Systems

Operational Security

- Insider Threats
- Recovery and Orchestration Failures

Risk #1

Backup Server Compromise

82% of Fortune 500 companies use Veeam, making backup servers high-value targets. Attackers specifically target backup systems to prevent recovery.

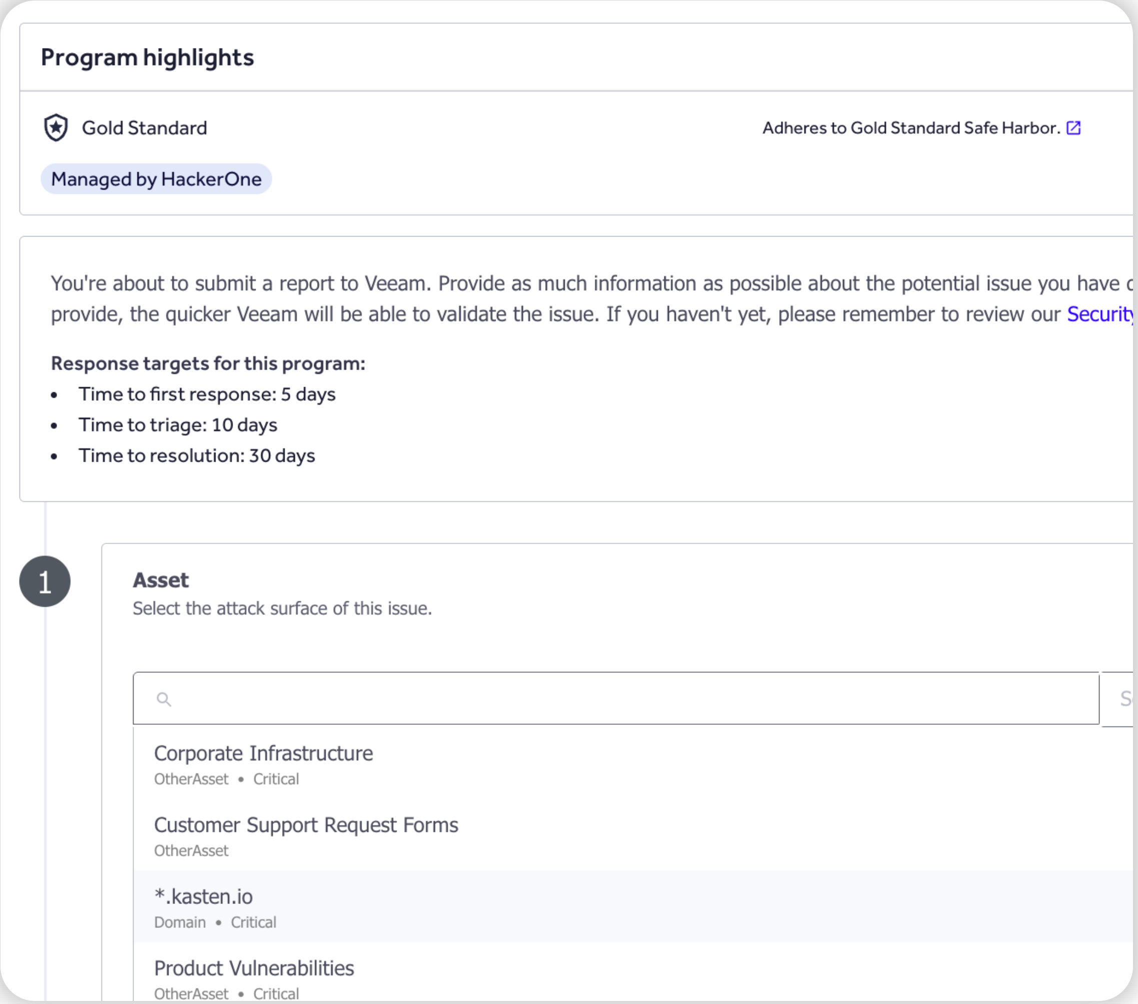
Backup Server Compromise

Vulnerarabilities in Veeam products

At Veeam we take software vulnerabilities in our products seriously.

We don’t just test our products; we scan, audit, and invite the world to help through our public [Vulnerability Disclosure Program](), anyone can report issues directly.

We’re committed to timely updates, clear communication, and constant improvement.



Program highlights

Gold Standard

Adheres to Gold Standard Safe Harbor.

Managed by HackerOne

You're about to submit a report to Veeam. Provide as much information as possible about the potential issue you have c provide, the quicker Veeam will be able to validate the issue. If you haven't yet, please remember to review our Security

Response targets for this program:

- Time to first response: 5 days
- Time to triage: 10 days
- Time to resolution: 30 days

1 **Asset**

Select the attack surface of this issue.

Corporate Infrastructure
OtherAsset • Critical

Customer Support Request Forms
OtherAsset

*.kasten.io
Domain • Critical

Product Vulnerabilities
OtherAsset • Critical

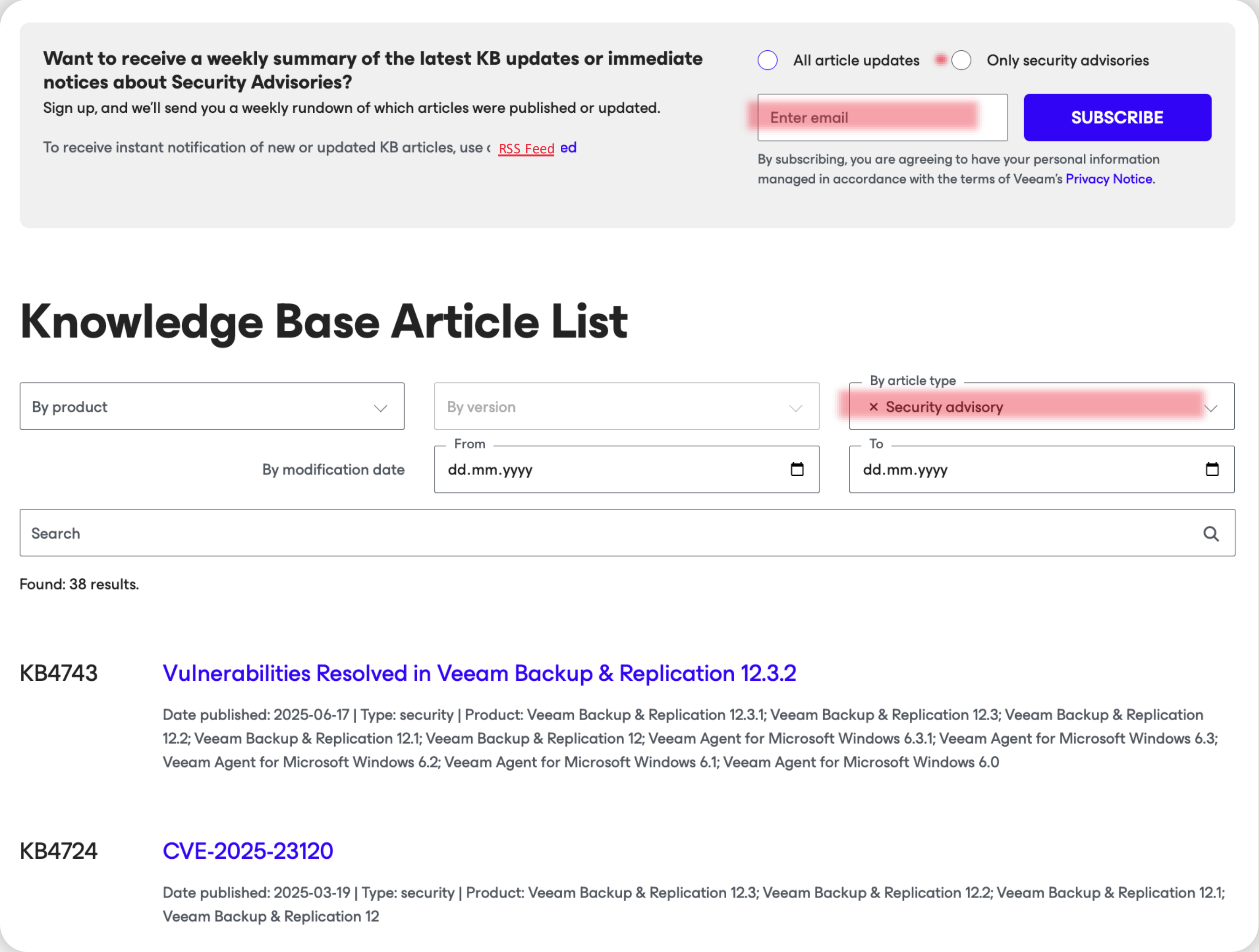
Backup Server Compromise

Stay up to date!

Vulnerabilities are a normal part of the cybersecurity landscape. Identifying and resolving them rapidly is crucial for your environment resiliency.

There is a dedicated “security advisory” list, where you can find detailed information about new vulnerabilities and critical updates. This list is regularly updated as new issues or patches emerge, helping act quickly.

It’s possible to subscribe to weekly email summaries of new and updated security advisories or to the RSS Feed for instant notifications.



Want to receive a weekly summary of the latest KB updates or immediate notices about Security Advisories?

Sign up, and we’ll send you a weekly rundown of which articles were published or updated.

To receive instant notification of new or updated KB articles, use (RSS Feed ed

○ All article updates ○ Only security advisories

Enter email

SUBSCRIBE

By subscribing, you are agreeing to have your personal information managed in accordance with the terms of Veeam’s Privacy Notice.

Knowledge Base Article List

By product | By version | By article type: × Security advisory

By modification date — From: dd.mm.yyyy — To: dd.mm.yyyy

Search

Found: 38 results.

KB4743 Vulnerabilities Resolved in Veeam Backup & Replication 12.3.2

Date published: 2025-06-17 | Type: security | Product: Veeam Backup & Replication 12.3.1; Veeam Backup & Replication 12.3; Veeam Backup & Replication 12.2; Veeam Backup & Replication 12.1; Veeam Backup & Replication 12; Veeam Agent for Microsoft Windows 6.3.1; Veeam Agent for Microsoft Windows 6.3; Veeam Agent for Microsoft Windows 6.2; Veeam Agent for Microsoft Windows 6.1; Veeam Agent for Microsoft Windows 6.0

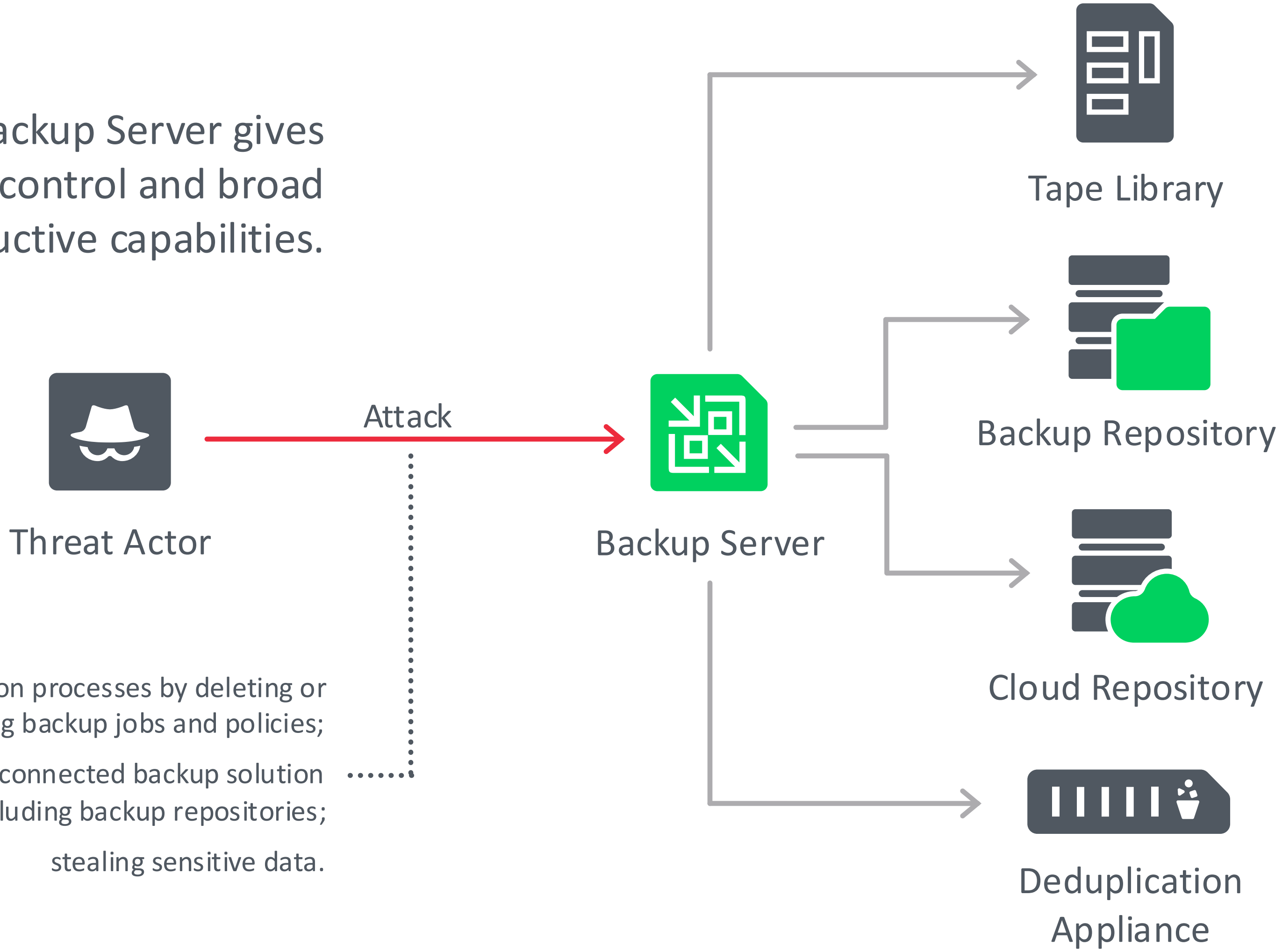
KB4724 CVE-2025-23120

Date published: 2025-03-19 | Type: security | Product: Veeam Backup & Replication 12.3; Veeam Backup & Replication 12.2; Veeam Backup & Replication 12.1; Veeam Backup & Replication 12

Backup Server Compromise

Resiliency Domains

Compromising the Backup Server gives attackers centralized control and broad destructive capabilities.



Interrupting data protection processes by deleting or disabling backup jobs and policies;

discovering all connected backup solution components, including backup repositories;

stealing sensitive data.

Backup Server Compromise

Security & Compliance Analyzer

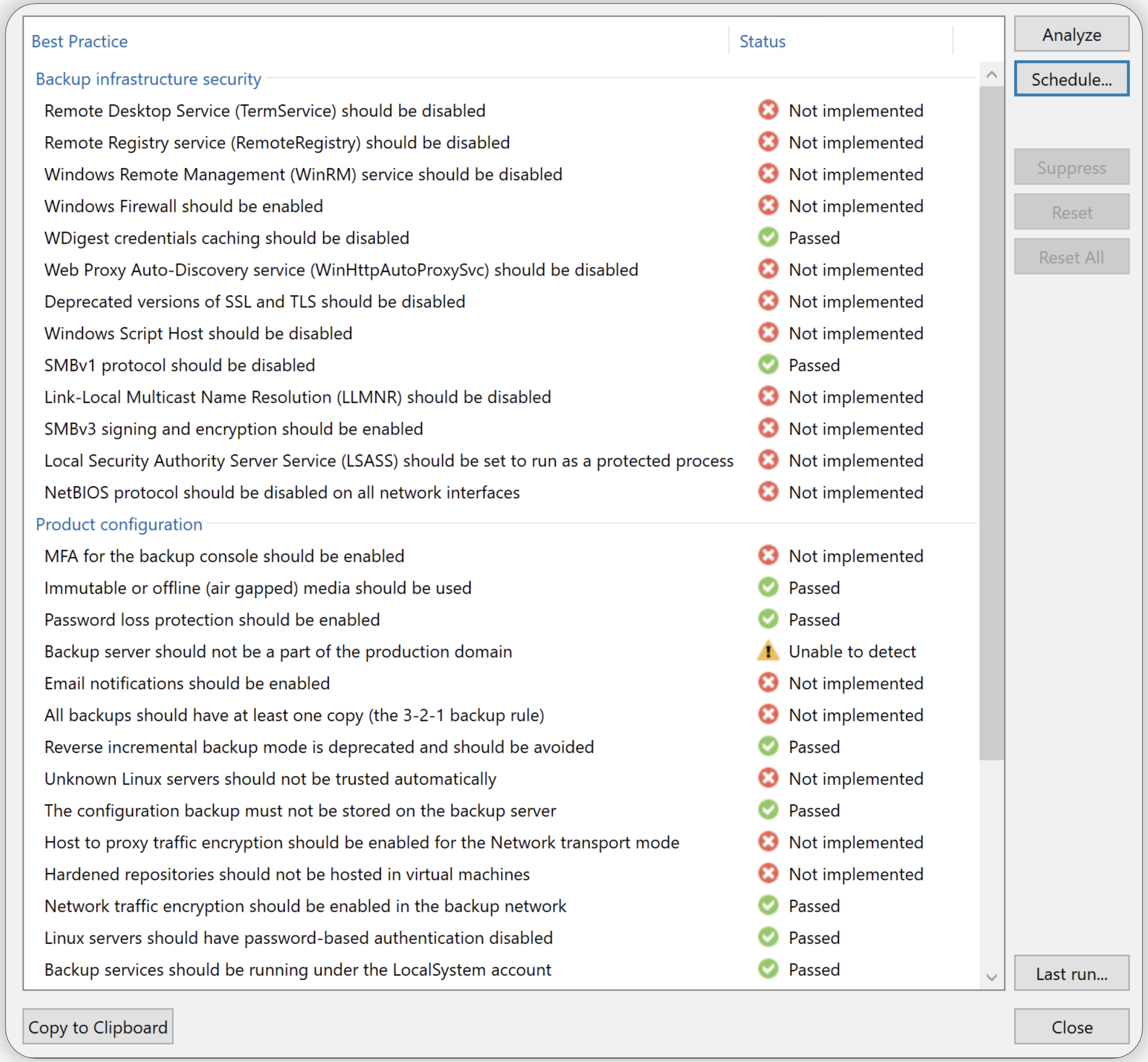
Security & Compliance Analyzer is a built-in feature in Veeam Backup & Replication.

This is a good starting point for hardening your environment.

By scanning your setup for security risks and compliance gaps, it offers actionable recommendations to improve resiliency and meet regulatory standards.

The Veeam Help Center provides a detailed description of each recommendation.

Also, there is a PowerShell script (KB4525) to automate the implementation of recommendations.



Best Practice	Status
Backup infrastructure security	
Remote Desktop Service (TermService) should be disabled	✗ Not implemented
Remote Registry service (RemoteRegistry) should be disabled	✗ Not implemented
Windows Remote Management (WinRM) service should be disabled	✗ Not implemented
Windows Firewall should be enabled	✗ Not implemented
WDigest credentials caching should be disabled	✓ Passed
Web Proxy Auto-Discovery service (WinHttpAutoProxySvc) should be disabled	✗ Not implemented
Deprecated versions of SSL and TLS should be disabled	✗ Not implemented
Windows Script Host should be disabled	✗ Not implemented
SMBv1 protocol should be disabled	✓ Passed
Link-Local Multicast Name Resolution (LLMNR) should be disabled	✗ Not implemented
SMBv3 signing and encryption should be enabled	✗ Not implemented
Local Security Authority Server Service (LSASS) should be set to run as a protected process	✗ Not implemented
NetBIOS protocol should be disabled on all network interfaces	✗ Not implemented
Product configuration	
MFA for the backup console should be enabled	✗ Not implemented
Immutable or offline (air gapped) media should be used	✓ Passed
Password loss protection should be enabled	✓ Passed
Backup server should not be a part of the production domain	⚠ Unable to detect
Email notifications should be enabled	✗ Not implemented
All backups should have at least one copy (the 3-2-1 backup rule)	✗ Not implemented
Reverse incremental backup mode is deprecated and should be avoided	✓ Passed
Unknown Linux servers should not be trusted automatically	✗ Not implemented
The configuration backup must not be stored on the backup server	✓ Passed
Host to proxy traffic encryption should be enabled for the Network transport mode	✗ Not implemented
Hardened repositories should not be hosted in virtual machines	✗ Not implemented
Network traffic encryption should be enabled in the backup network	✓ Passed
Linux servers should have password-based authentication disabled	✓ Passed
Backup services should be running under the LocalSystem account	✓ Passed

Backup Server Compromise

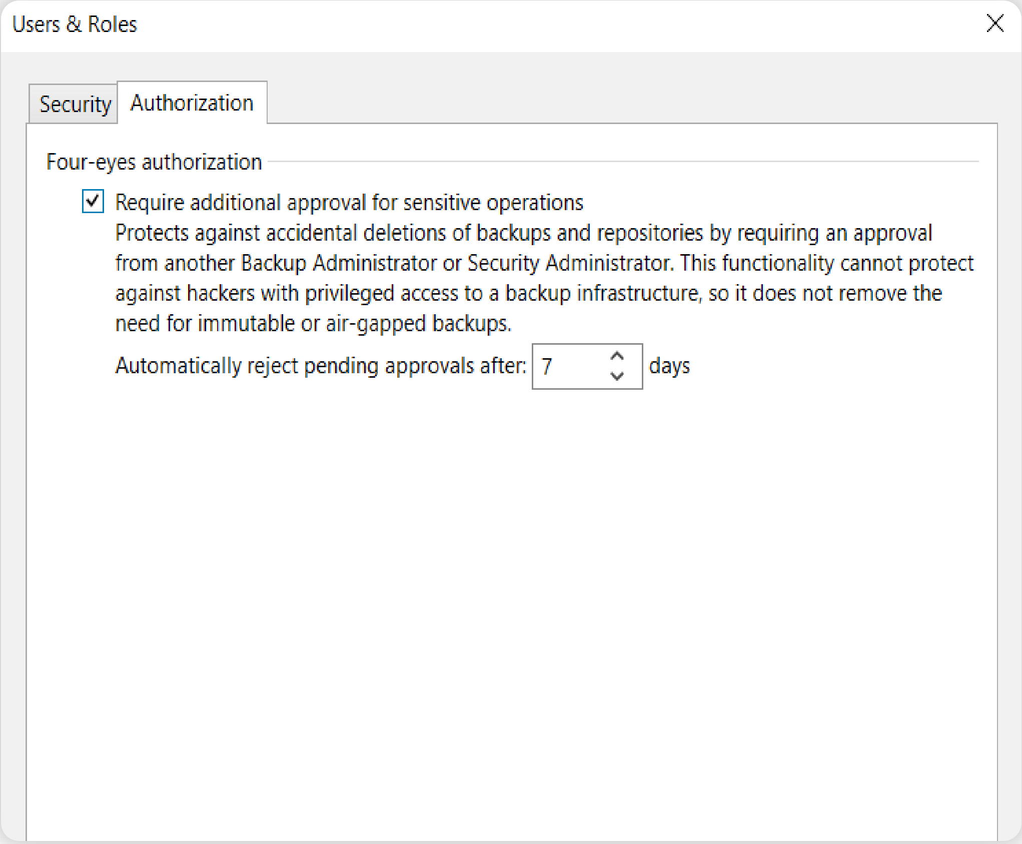
Security & Compliance Analyzer

Here are some impactful recommendations for Backup Server hardening:

- Make sure that Veeam Backup & Replication (VBR) server is not a part of Active Directory domain. Running the VBR server in a workgroup reduces the attack surface and limits lateral movement in case domain credentials are compromised.
- Enforce MFA for access to the VBR console. This significantly increases protection against unauthorized logins, even if account credentials are stolen or guessed.
- Enable Four-Eyes Authorization that requires two authorized individuals to approve sensitive operations.
- Use “Security Officer” feature (available in Veeam Software Appliance). A role that approves requests for access elevation and other sensitive operations.
- Disable RDP where possible or tightly restrict RDP access to the VBR server. If RDP is necessary, limit access to trusted IP addresses and use network-level authentication to reduce exposure to brute-force and remote attacks.

Backup Server Compromise

MFA & Four-eyes

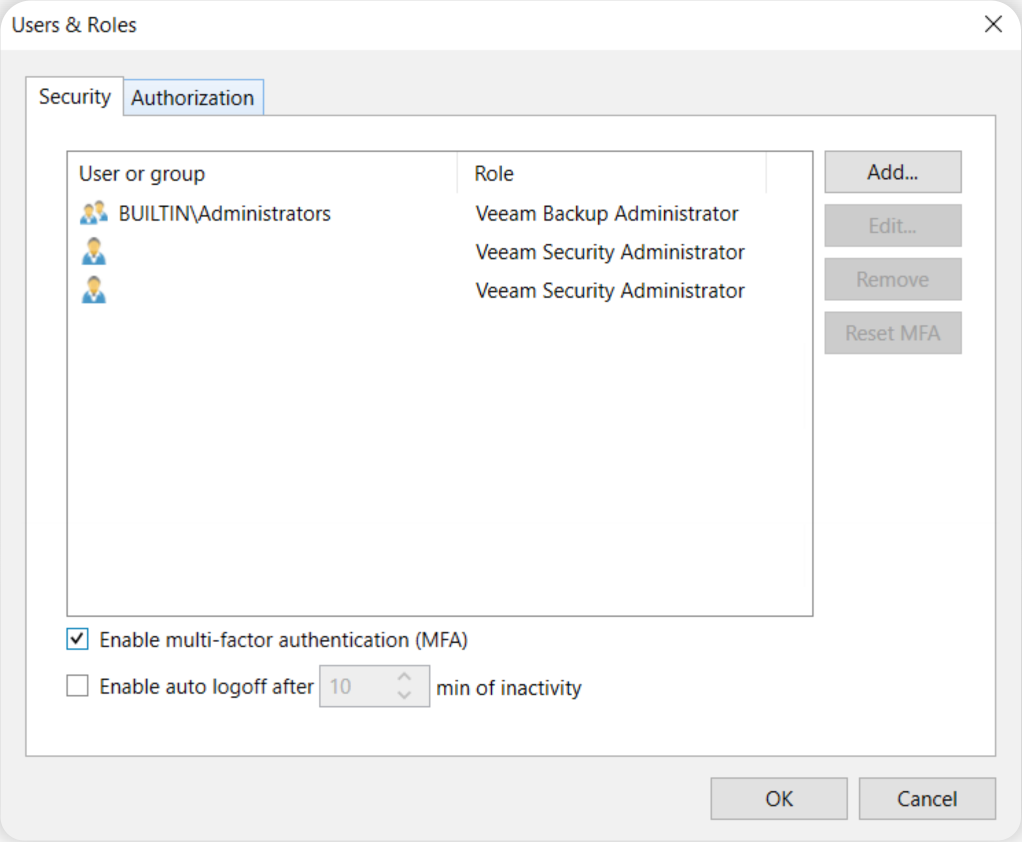


Four-eyes authorization

☑ Require additional approval for sensitive operations

Protects against accidental deletions of backups and repositories by requiring an approval from another Backup Administrator or Security Administrator. This functionality cannot protect against hackers with privileged access to a backup infrastructure, so it does not remove the need for immutable or air-gapped backups.

Automatically reject pending approvals after: 7 days



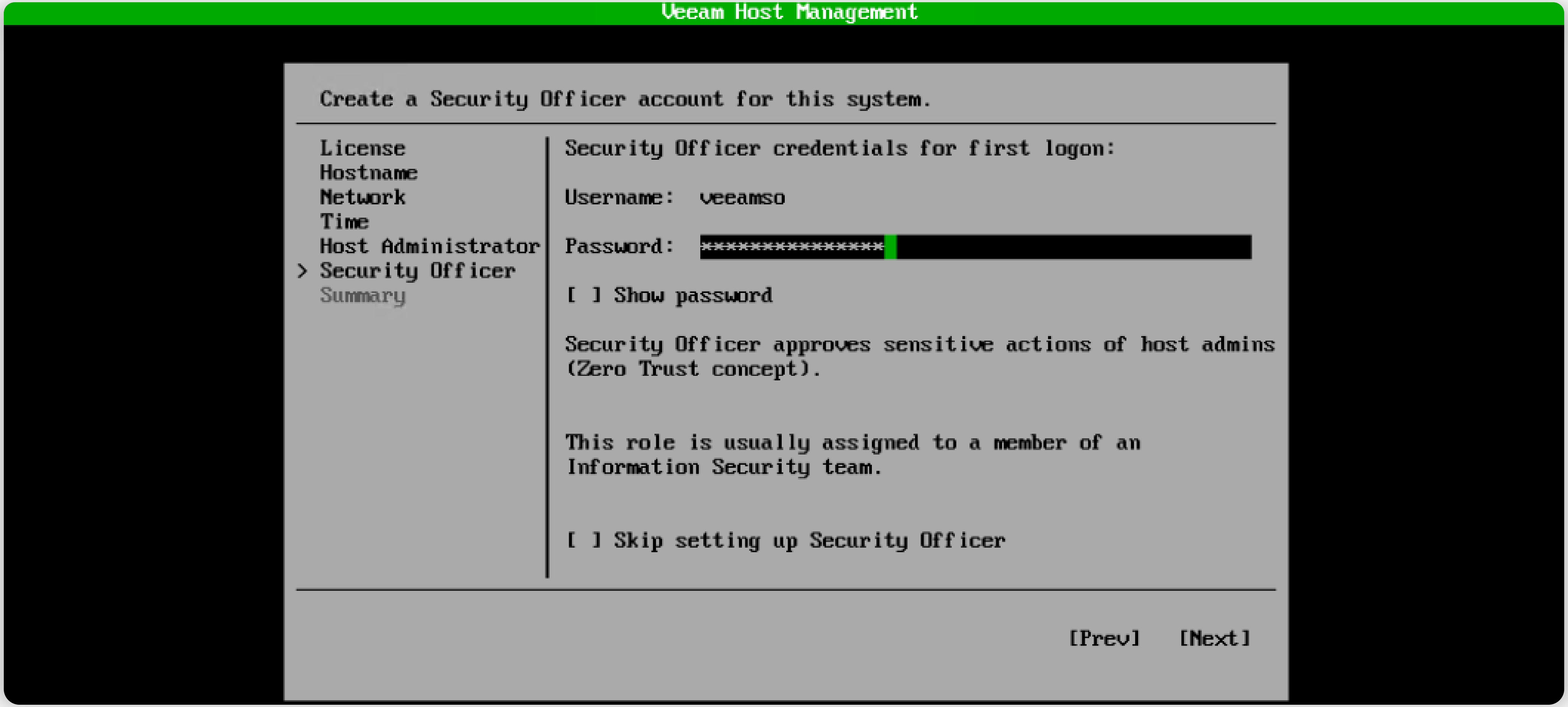
User or group	Role
BUILTIN\Administrators	Veeam Backup Administrator
	Veeam Security Administrator
	Veeam Security Administrator

☑ Enable multi-factor authentication (MFA)

□ Enable auto logoff after 10 min of inactivity

Backup Server Compromise

Security Officer (Veeam Software Appliance)



Veeam Host Management

Create a Security Officer account for this system.

Security Officer credentials for first logon:

Username: veeamso

Password: ****************

[ ] Show password

Security Officer approves sensitive actions of host admins (Zero Trust concept).

This role is usually assigned to a member of an Information Security team.

[ ] Skip setting up Security Officer

Backup Server Compromise

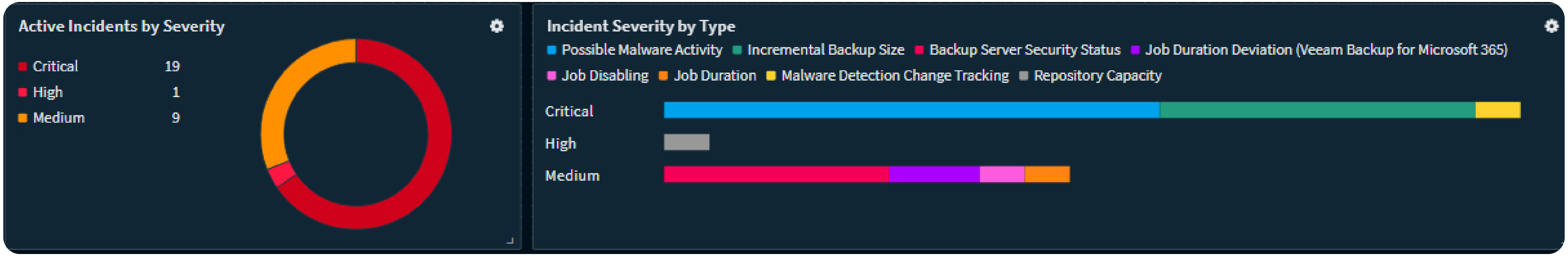
Be informed: Security Information Event Management (SIEM)

10 Critical Alarms to Stop Ransomware and Protect Your Business Continuity

300+ events are available through RFC 5424 Syslog Integration, such as:

- MFA Attempts Exceeded Alarm
- Suspicious Ransomware Activity Alarm
- Attempted Backup Deletions
- Malware Activity Detected

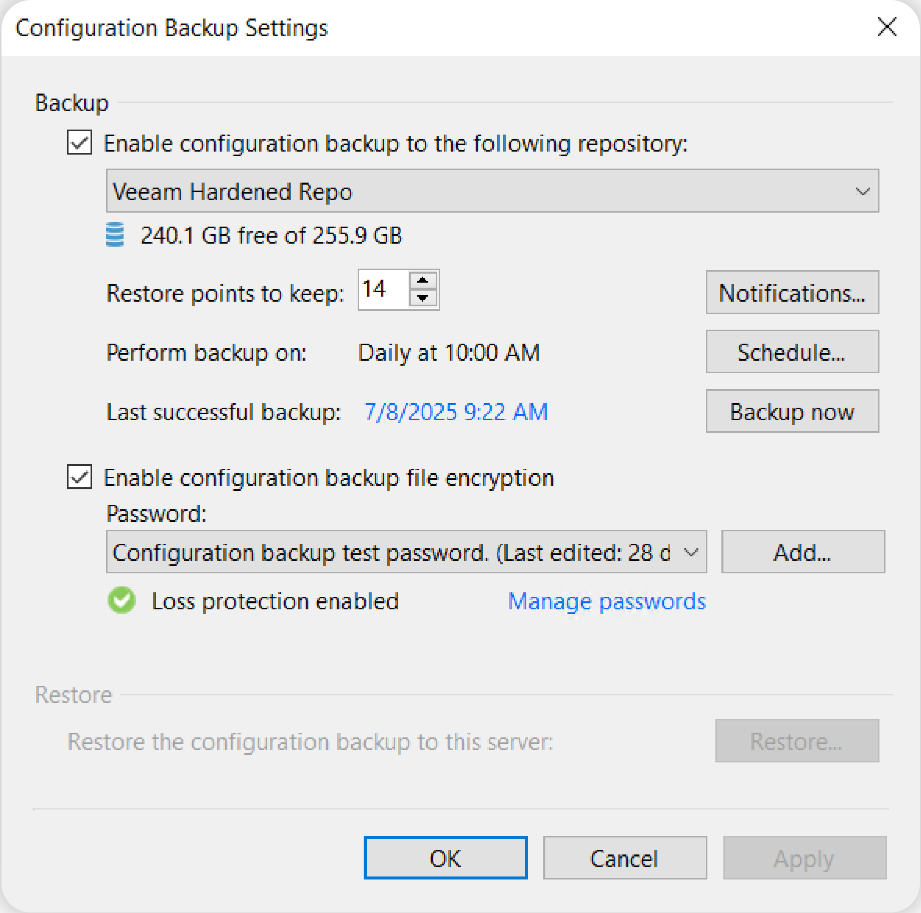
splunk> CROWDSTRIKE FORTINET paloalto NETWORKS SOPHOS


Active Incidents by Severity
🟥 Critical 19
🟥 High 1
🟧 Medium 9
Incident Severity by Type
Possible Malware Activity
Incremental Backup Size
Backup Server Security Status
Job Duration Deviation (Veeam Backup for Microsoft 365)
Job Disabling
Job Duration
Malware Detection Change Tracking
Repository Capacity
Critical
High
Medium

Backup Server Compromise

Configuration Backup

- Configuration database backup is the way how VBR “backs itself up”
- Encrypt data in configuration backups with the secure password
- Store configuration backups in a secure and immutable location
- Follow the 3-2-1 backup design framework
- Schedule regular configuration backups to ensure up-to-date recovery points



Configuration Backup Settings

Backup

☑ Enable configuration backup to the following repository:

Veeam Hardened Repo

240.1 GB free of 255.9 GB

Restore points to keep: 14

Perform backup on: Daily at 10:00 AM

Last successful backup: 7/8/2025 9:22 AM

☑ Enable configuration backup file encryption

Password:

Configuration backup test password. (Last edited: 28 d

Loss protection enabled

Restore

Restore the configuration backup to this server:

Backup Server Compromise

Data Exfiltration

Data Exfiltration is unauthorized data theft from backup or production environments.

Attackers frequently exfiltrate data before deploying ransomware to increase leverage over victims – threatening to leak or sell stolen information if ransom is unpaid. This tactic amplifies risk not only of data loss but also of privacy breaches, reputational damage, and regulatory penalties.

Indicators of Compromise Tools Scanner and Threat Hunter can help to identify signs of exfiltration tools or suspicious activity.

By encrypting backups during transport across networks and while stored, Veeam ensures that even if attackers intercept or access the data, they cannot easily read or misuse it.

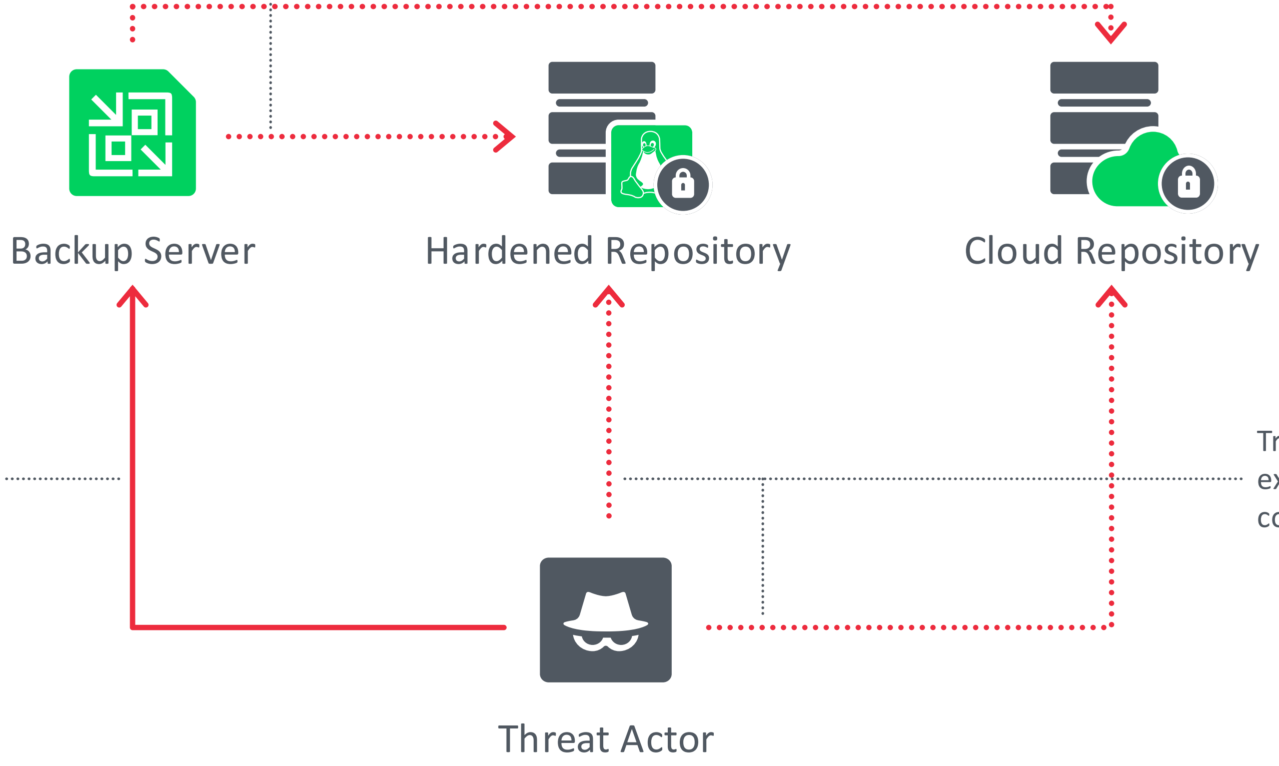
Risk #2

Backup Data Encryption/Deletion

Statistics: 89% of organizations had their backup repositories targeted and more than one-third saw critical backup data modified or destroyed.

Backup Data Encryption/Deletion Prevention

Resiliency Domains



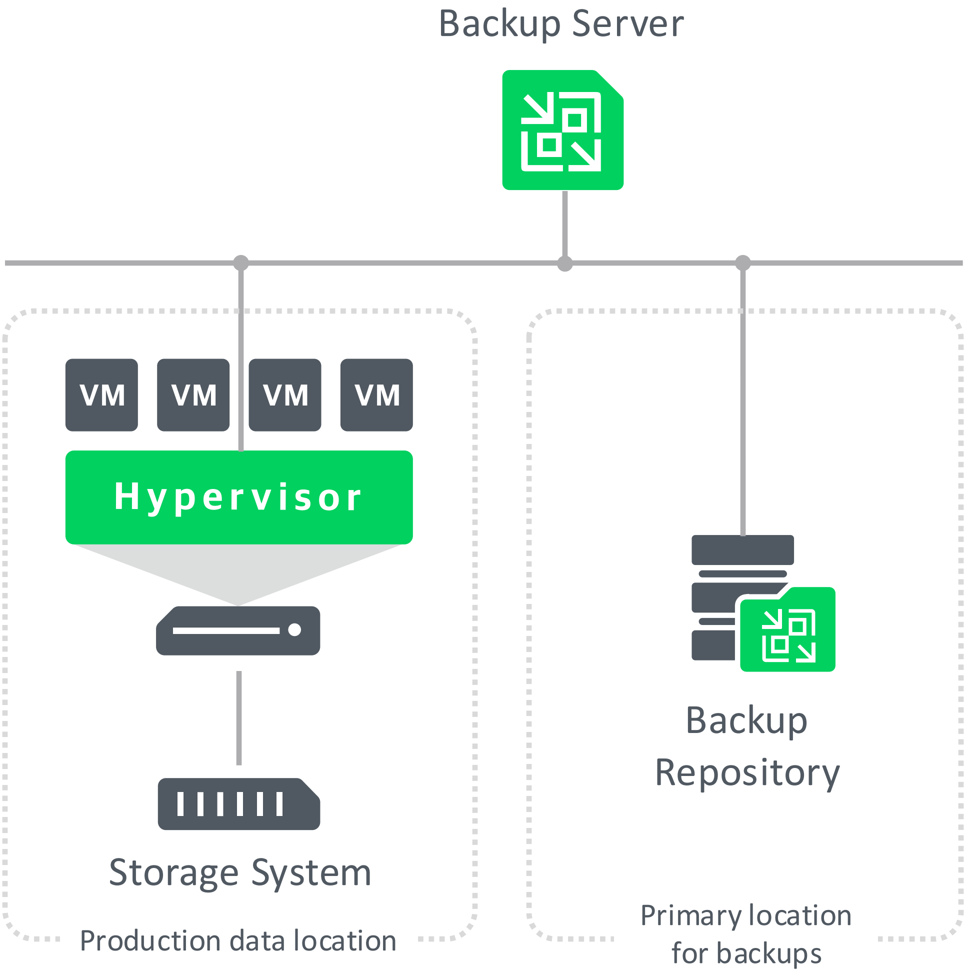
Try to delete backups from
the management console

Compromise backup server;
Identify backup solution components;
Disable or delete backup jobs;

Try to wipe backups by using
exploits, vulnerabilities,
compromised credentials, etc.

Backup Data Encryption/Deletion Prevention

3-2-1 rule

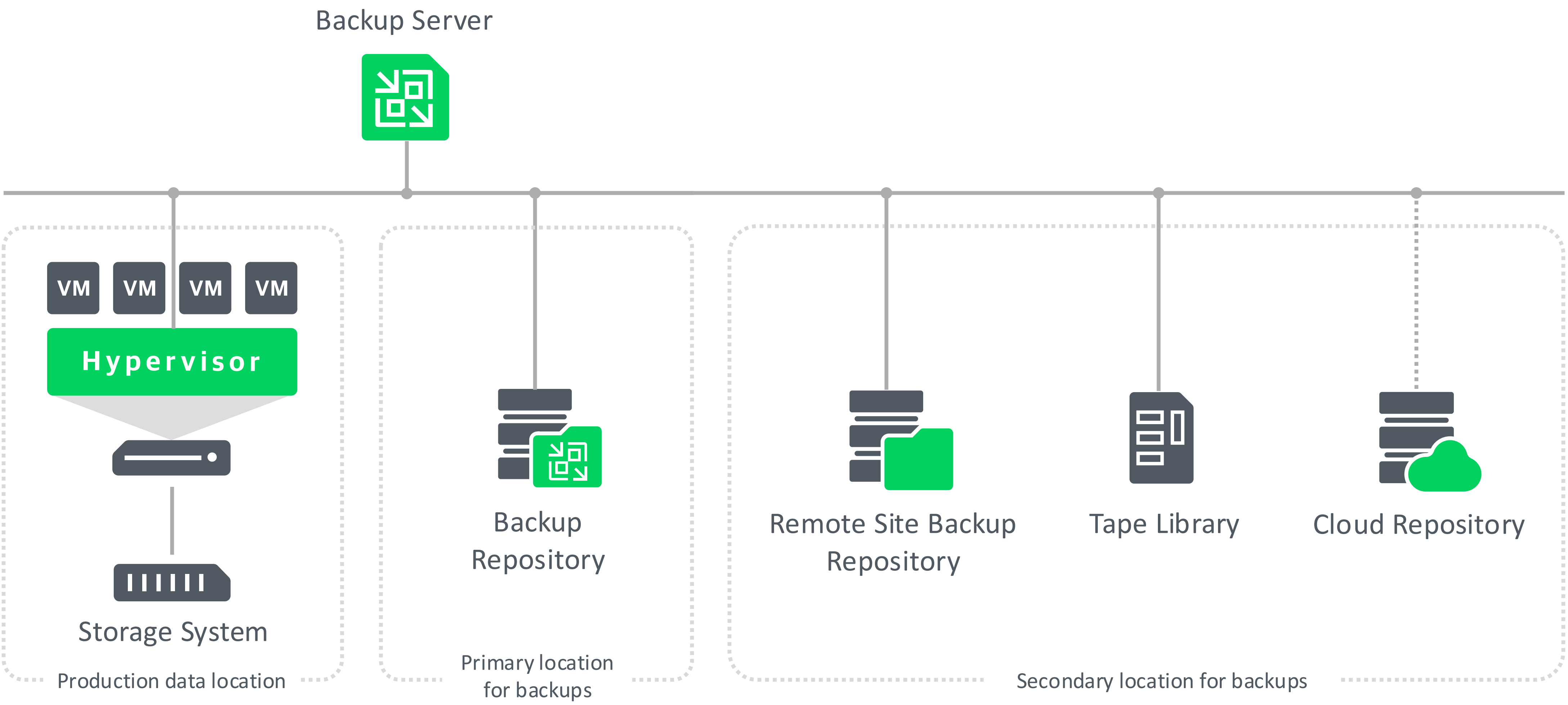


By maintaining multiple copies on different types of media and keeping at least one copy off-site, the rule ensures there is no single point of failure, making data loss much less likely.

If one copy is lost, damaged or compromised due to hardware failure, human error or cyberattack, you still have other copies available to restore your information.

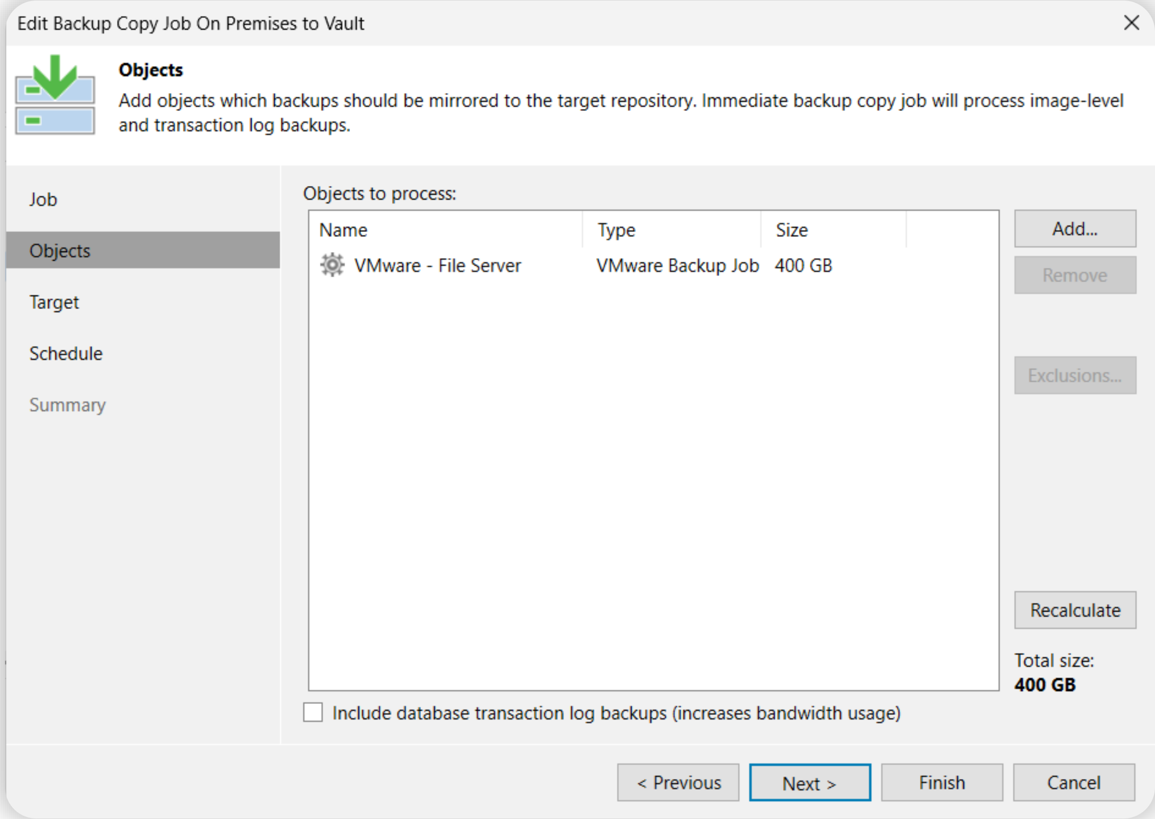
Backup Data Encryption/Deletion Prevention

3-2-1 rule



Backup Data Encryption/Deletion Prevention

Backup Copy Job



Edit Backup Copy Job On Premises to Vault

Objects

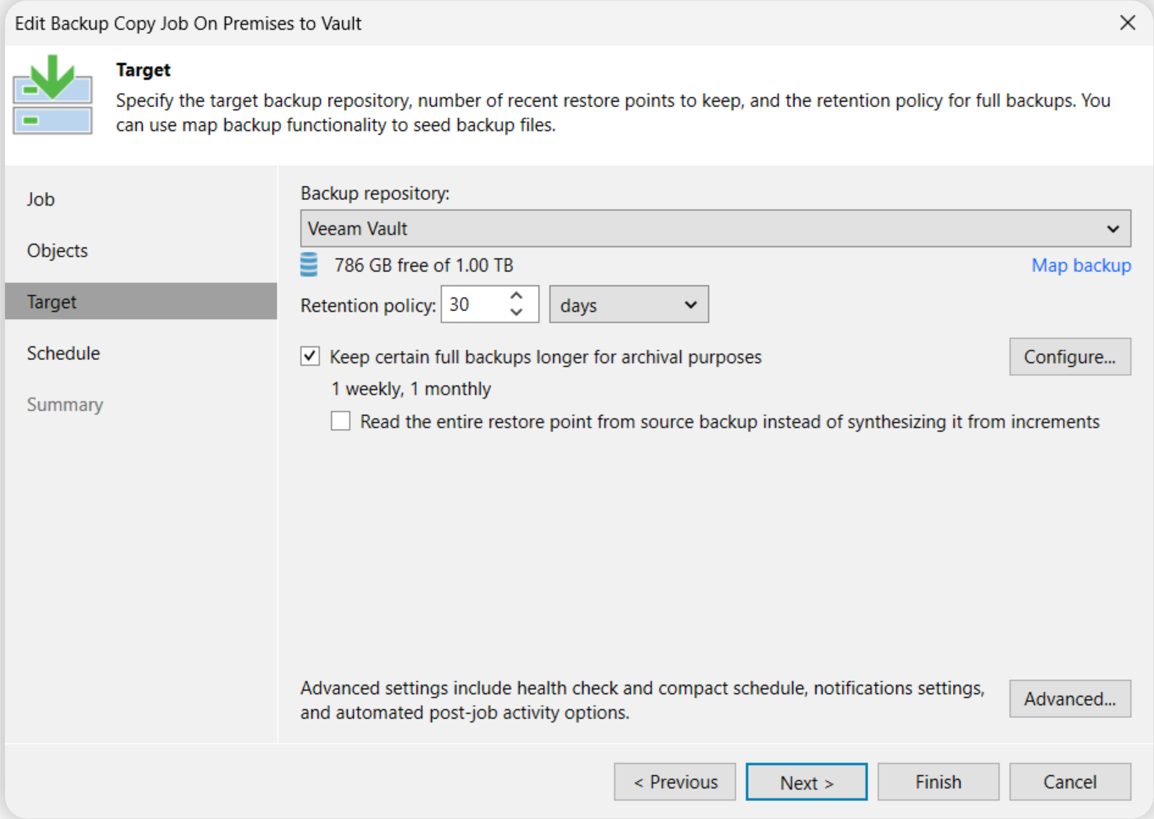
Add objects which backups should be mirrored to the target repository. Immediate backup copy job will process image-level and transaction log backups.

Objects to process:

Name	Type	Size
VMware - File Server	VMware Backup Job	400 GB

Total size:
400 GB

□ Include database transaction log backups (increases bandwidth usage)



Edit Backup Copy Job On Premises to Vault

Target

Specify the target backup repository, number of recent restore points to keep, and the retention policy for full backups. You can use map backup functionality to seed backup files.

Backup repository: Veeam Vault

786 GB free of 1.00 TB

Retention policy: 30 days

☑ Keep certain full backups longer for archival purposes

1 weekly, 1 monthly

□ Read the entire restore point from source backup instead of synthesizing it from increments

Advanced settings include health check and compact schedule, notifications settings, and automated post-job activity options.

Backup Data Encryption/Deletion Prevention

Immutability

Definition of Immutability:

- Immutability refers to the state of data that prevents it from being modified or deleted.

Benefits of Immutability:

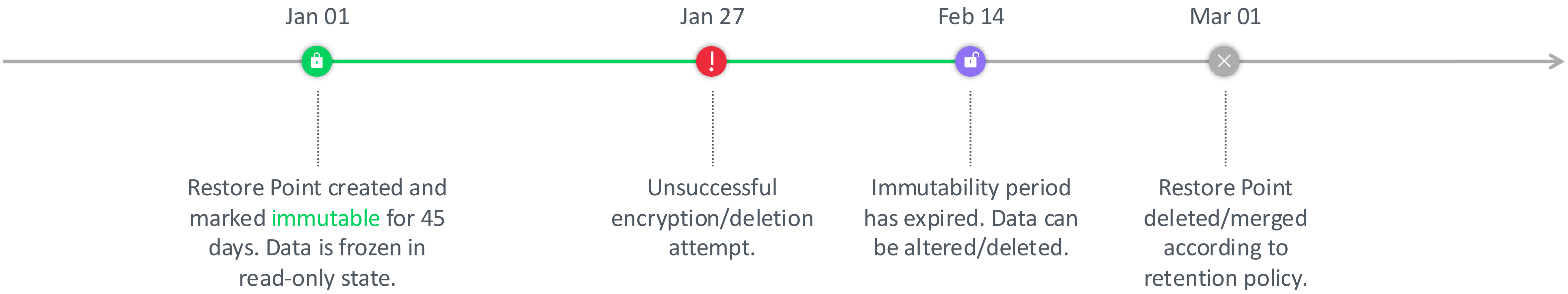
- Ensures data integrity and security.
- Provides protection against ransomware and accidental deletions.

Supported types of immutable repositories

- Veeam Hardened Repository
- Veeam Data Cloud Vault
- Amazon, Azure, Google Cloud Storage and other S3-compatible object storage repositories
- HPE StoreOnce
- Dell EMC Data Domain

Backup Data Encryption/Deletion Prevention

Immutability timeline



Jan 01

Restore Point created and marked immutable for 45 days. Data is frozen in read-only state.

Jan 27

Unsuccessful encryption/deletion attempt.

Feb 14

Immutability period has expired. Data can be altered/deleted.

Mar 01

Restore Point deleted/merged according to retention policy.

Backup Data Encryption/Deletion Prevention

Hardened Repository

A hardened repository is a secure storage with the immutability support designed to protect backup data from deletion, alteration or attacks (like ransomware), even if someone gains unauthorized access.

- Can run on generic Linux, eliminating vendor lock-in and enabling organizations to choose their preferred hardware or Linux distribution (such as Ubuntu, Debian, RHEL, SLES, Rocky, etc.).

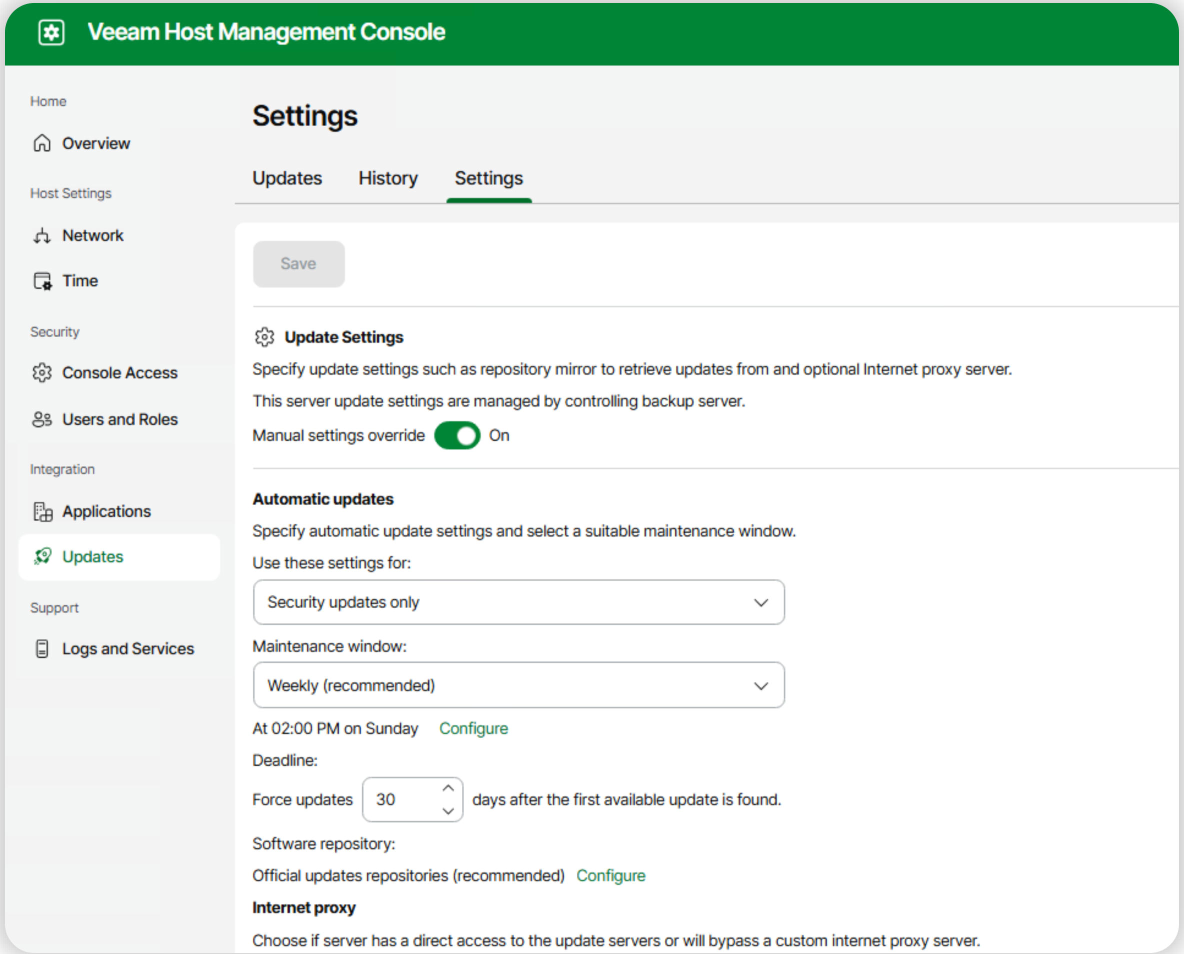
  The machine must meet system requirements for backup repositories, and there are additional requirements/limitations for the Hardened Repository.

- Can be installed from Veeam maintained Hardened Repository ISO (JeOS + Repository packages). JeOS manages and updates the OS and Veeam components, simplifying maintenance with automatic patching.

  Hardware must be on the Red Hat compatibility list or CIQ certified hardware list.

Backup Data Encryption/Deletion Prevention

JeOS Host Management Console



Update Settings

Specify update settings such as repository mirror to retrieve updates from and optional Internet proxy server.

This server update settings are managed by controlling backup server.

Manual settings override: On

Automatic updates

Specify automatic update settings and select a suitable maintenance window.

Use these settings for: Security updates only

Maintenance window: Weekly (recommended)

At 02:00 PM on Sunday Configure

Deadline:

Force updates 30 days after the first available update is found.

Software repository:

Official updates repositories (recommended) Configure

Internet proxy

Choose if server has a direct access to the update servers or will bypass a custom internet proxy server.

- Customized version of minimal Rocky Linux
- Simple and fast deployment
- Pre-hardened with DISA-STIG Security Profile
- Fully automated vulnerability patching
- MFA is mandatory

Backup Data Encryption/Deletion Prevention

Hardened Repository Features

- Immutable backups: Files are protected against modification and deletion for a user-defined period, even if administrative credentials are compromised. This ensures backups cannot be altered or deleted by malware, ransomware, or accidental administrator actions.

- Air-gapped-like protection: The repository is hardened by limiting access and disabling protocols like SSH, minimizing the attack surface and acting as an “impenetrable black box” for backup files.

- Protection against insider threats: By using single-use credentials and disabling root access for backup processes, the repository mitigates risks even if the main Veeam server is breached.

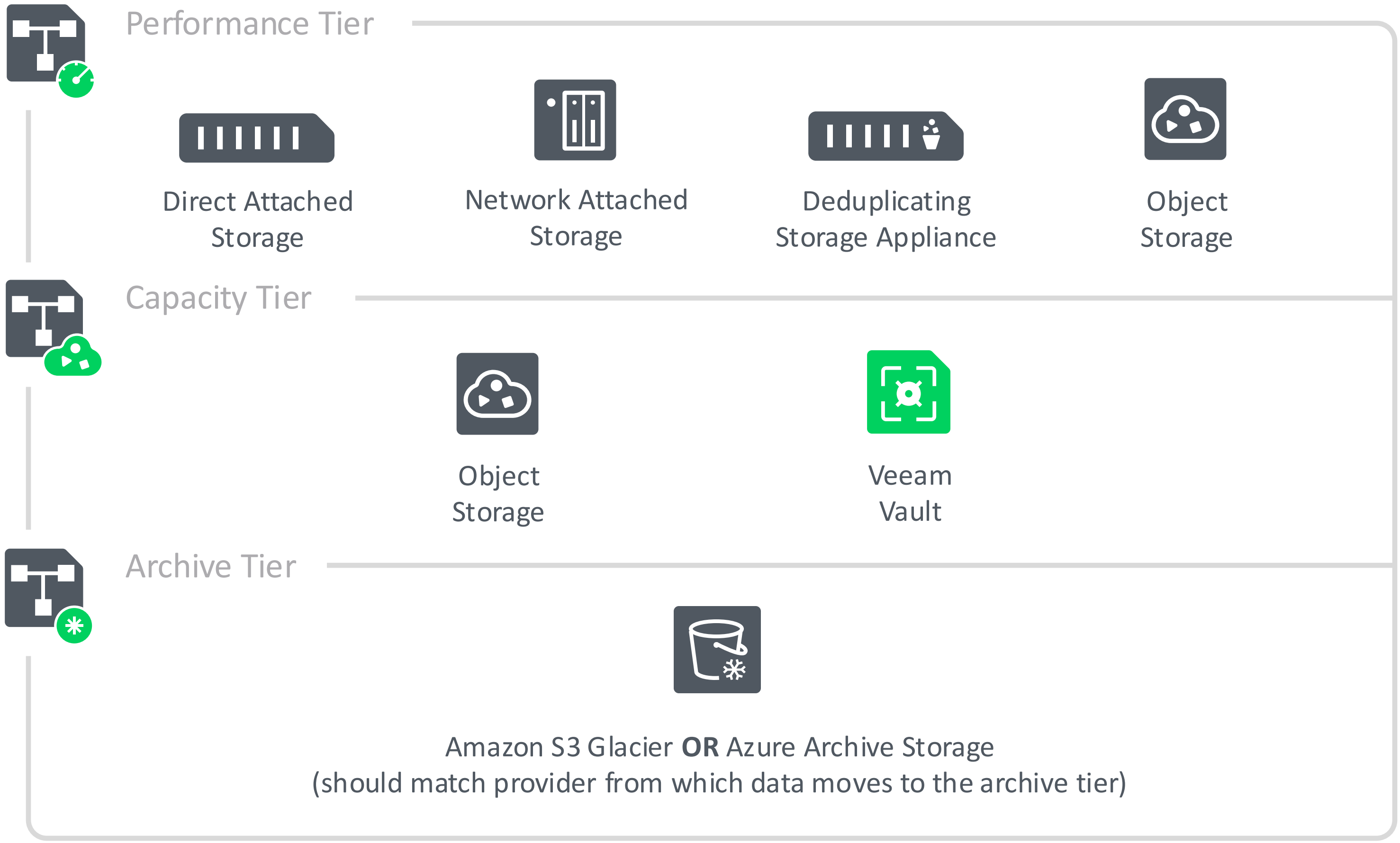
- Space efficiency: When paired with the XFS file system, benefits from block cloning technology for efficient synthetic full backups, reduced disk usage, and faster backup operations.

Backup Data Encryption/Deletion Prevention

Scale–Out Backup Repository (SOBR)

A scalable repository system with multi–tier storage support.

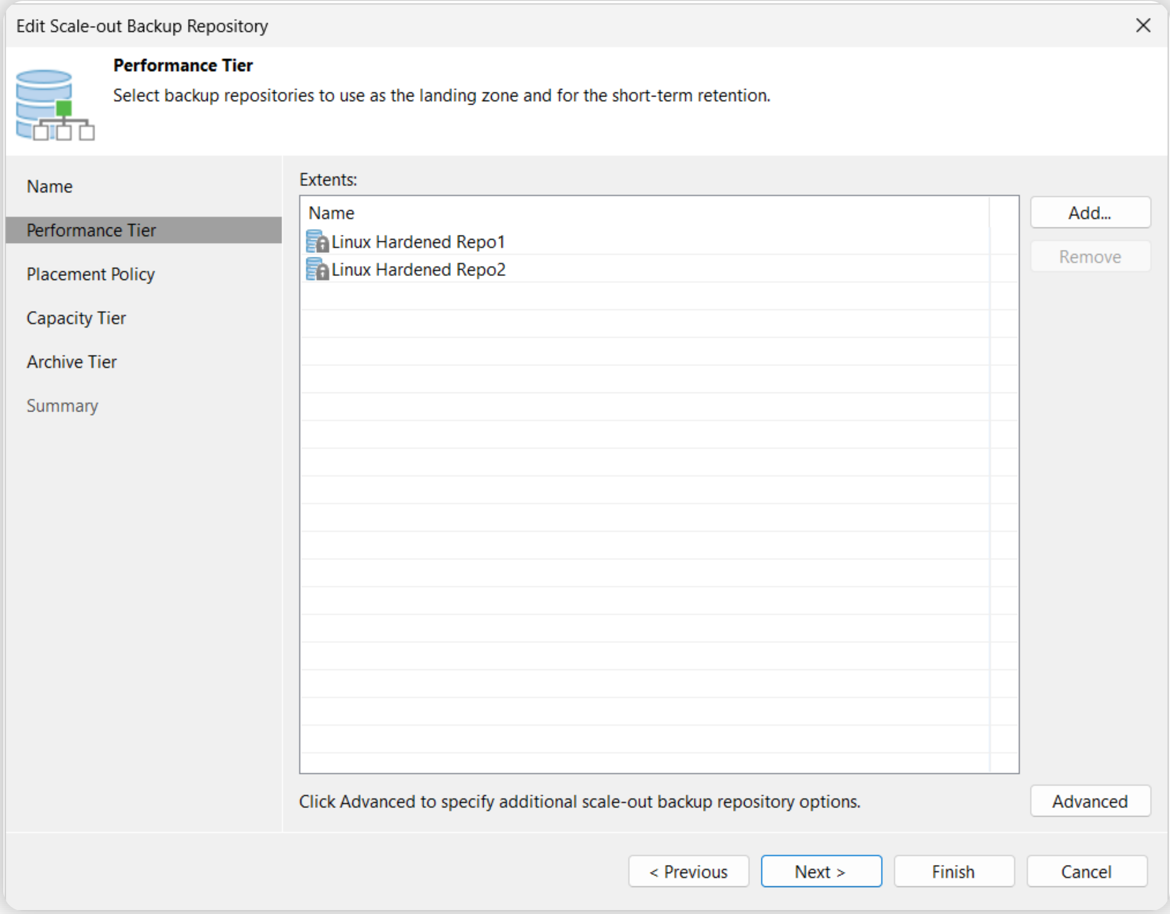
Includes performance tier (local or shared storage) and can be extended with capacity and archive tiers, providing horizontal scaling for diverse storage needs.



Amazon S3 Glacier **OR** Azure Archive Storage
(should match provider from which data moves to the archive tier)

Backup Data Encryption/Deletion Prevention

SOBR: Performance Tier



Edit Scale-out Backup Repository

Performance Tier

Select backup repositories to use as the landing zone and for the short-term retention.

Extents:

Name
Linux Hardened Repo1
Linux Hardened Repo2

Click Advanced to specify additional scale-out backup repository options.

The Performance Tier consists of one or more backup repositories called extents

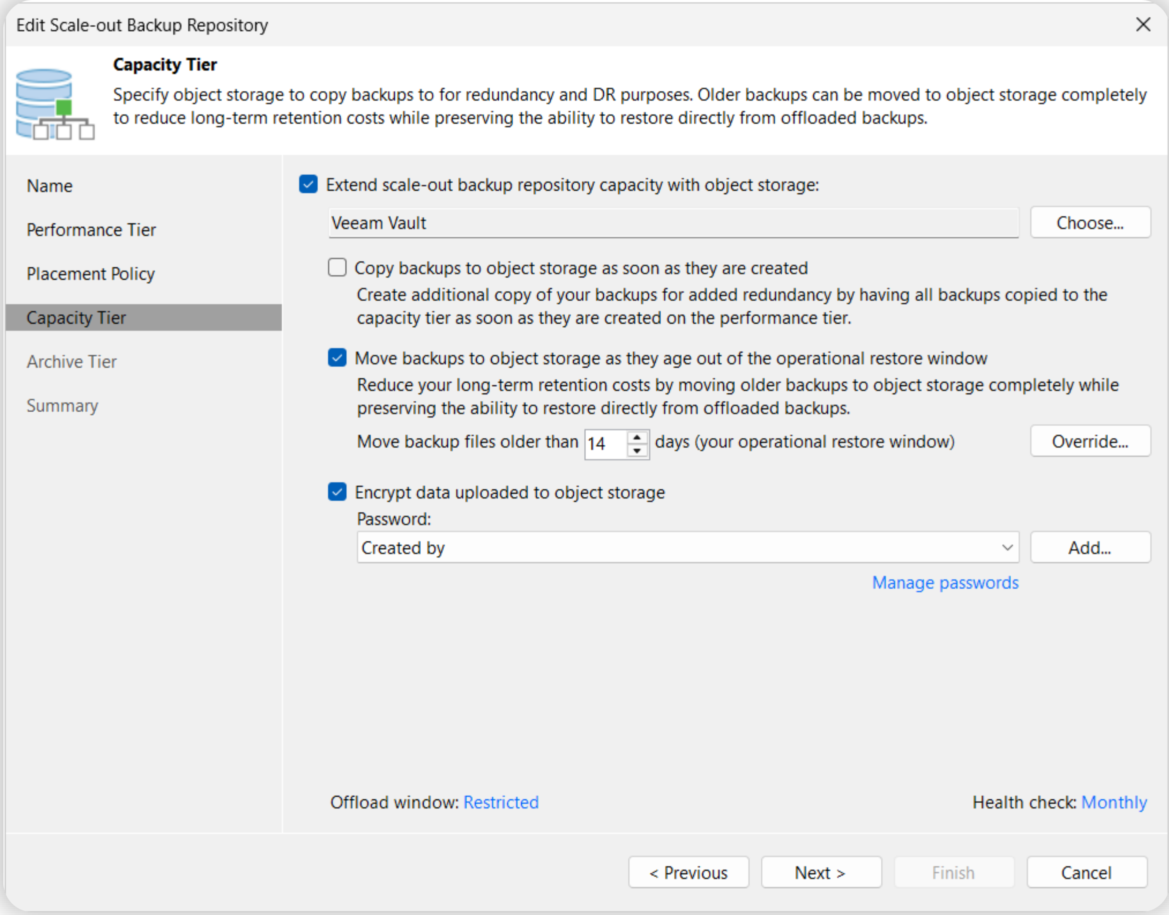
Extents combine seamlessly to form a single scalable backup target

Supports immutability settings on compatible extents to protect backups from ransomware and accidental deletion

Acts as the primary backup storage that holds recent data for fast recovery while integrating with Capacity Tier for offloading backups

Backup Data Encryption/Deletion Prevention

SOBR: Capacity Tier



Edit Scale-out Backup Repository

Capacity Tier

Specify object storage to copy backups to for redundancy and DR purposes. Older backups can be moved to object storage completely to reduce long-term retention costs while preserving the ability to restore directly from offloaded backups.

☑ Extend scale-out backup repository capacity with object storage:

Veeam Vault

□ Copy backups to object storage as soon as they are created

Create additional copy of your backups for added redundancy by having all backups copied to the capacity tier as soon as they are created on the performance tier.

☑ Move backups to object storage as they age out of the operational restore window

Reduce your long-term retention costs by moving older backups to object storage completely while preserving the ability to restore directly from offloaded backups.

Move backup files older than 14 days (your operational restore window)

☑ Encrypt data uploaded to object storage

Password: Created by

Offload window: Restricted

Health check: Monthly

The Capacity Tier is an additional storage layer designed for cost-effective and longer-term retention, typically cloud-based

Automatically moves or copies backups from Performance Tier to Capacity Tier

Capacity Tier supports immutable backups via object-locking capabilities to safeguard data integrity

By separating Performance Tier from Capacity Tier, it ensures you maintain multiple backup copies across different media and locations

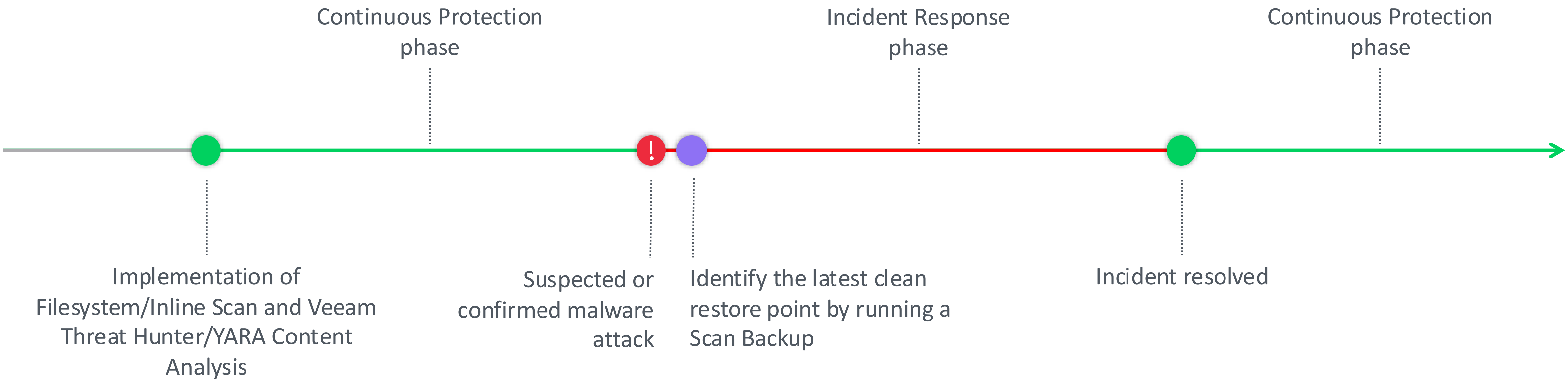
Risk #3

Malware in Backups

Restoring from an infected backup can reintroduce malware into the production environment, resulting in reinfection cycles and potential data corruption across systems.

Malware in Backups

Simplified Workflow



Continuous Protection phase

Incident Response phase

Continuous Protection phase

Implementation of Filesystem/Inline Scan and Veeam Threat Hunter/YARA Content Analysis

Suspected or confirmed malware attack

Identify the latest clean restore point by running a Scan Backup

Incident resolved

Malware in Backups

How to detect Malware?

File system activity analysis – used during the backup job scans guest indexing data for: known suspicious files and extensions, deleted files, extension changes.

Indicators of Compromise Tools Scanner – Indicators of compromise are non-malware programs. However, their unexpected presence on a system can indicate a security risk.

Inline Scan (entropy analysis) – scans blocks in data stream during backup job for: files encrypted by malware, artifacts created by malware like onion links, notes created by Medusa and Clop.

Signature-based detection (Veeam Threat Hunter) – can be used during Scan Backup, Secure Restore and SureBackup. An alternative to third-party antivirus that can be integrated with VBR. Using a signature-based detection engine, such as antivirus, in the production environment and another (Veeam Threat Hunter) with a different set of malware definitions for backups is a good practice. Marks infected objects.

Rule-based detection (YARA) – like a signature-based detection, can be used during Scan Backup, Secure Restore and SureBackup. Allows to create custom rules for identifying malware based on textual or binary pattern. Marks infected objects.

Third-party solutions – it's possible to use Veeam Incident API to send a request about detected malware activity to Veeam Backup & Replication and mark a machine as infected.

Malware in Backups

When and how use these features?

When?	During the Backup Job		On-demand	Before restore	During the backup recovery verification
What?	Guest Indexing Data Scan	Inline Scan	Scan Backup	Secure Restore	SureBackup
How?	Filesystem activity analysis. Scans guest indexing data for: known suspicious files and extensions, deleted files, extension changes, non-malware programs that can indicate a security risk (Indicators of Compromise Tools Scanner).	Entropy analysis. Scans blocks in data stream during the Backup Job for: files encrypted by malware, artifacts created by malware like onion links, notes created by Medusa and Clop.	A Signature-based detection (Veeam Threat Hunter) and/or Rule-based detection (YARA Scan) can be used after malware attack to find latest clean restore point or to find a sensitive data in the backups.	Veeam Threat Hunter and/or YARA Scan can be used to scan machine data for malware activity before restoring the machine to the production environment.	Veeam Threat Hunter and/or YARA Scan can be used during the SureBackup Job to proactively protect against the risk of restoring compromised data into your production environment.

Malware in Backups

Why Veeam Threat Hunter is recommended over third-party AV?

- Automatically installed on each mount server
- 3-6x times faster than Windows Defender
- Uses signatures that are more specific for backups
- Similar to AV CPU and RAM utilization, despite higher throughput
- Proprietary engine with no user-modifiable signatures
- Included in Veeam Data Platform Advanced: no additional AV license fees

Switching to a third-party AV solution is always an option if you desire.

Malware in Backups

YARA Rules Guide: What They Are and How to Write Them

What is YARA and how to create YARA rules?

```
rule RuleName {
  meta:
    author = "Security Team"
    description = "Custom threat detection"
    date = "2025-06-30"

  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)
}
```

Malware in Backups

Where to find ready to use YARA rules?

Public repositories

There are plenty of community driven repositories. Some of them are updated quite often. Just google it or ask your favorite AI.

Some considerations:

- Not all public rules maintain the same quality standards. Organizations should validate rules against both malicious samples and clean files to minimize false positives before deployment.
- Complex rules with multiple conditions can significantly slow scanning performance. For example: rules should avoid short strings (less than 4 bytes), minimize wildcards in hex strings, and use regex sparingly with fixed 4-byte anchors.

Generators and LLMs

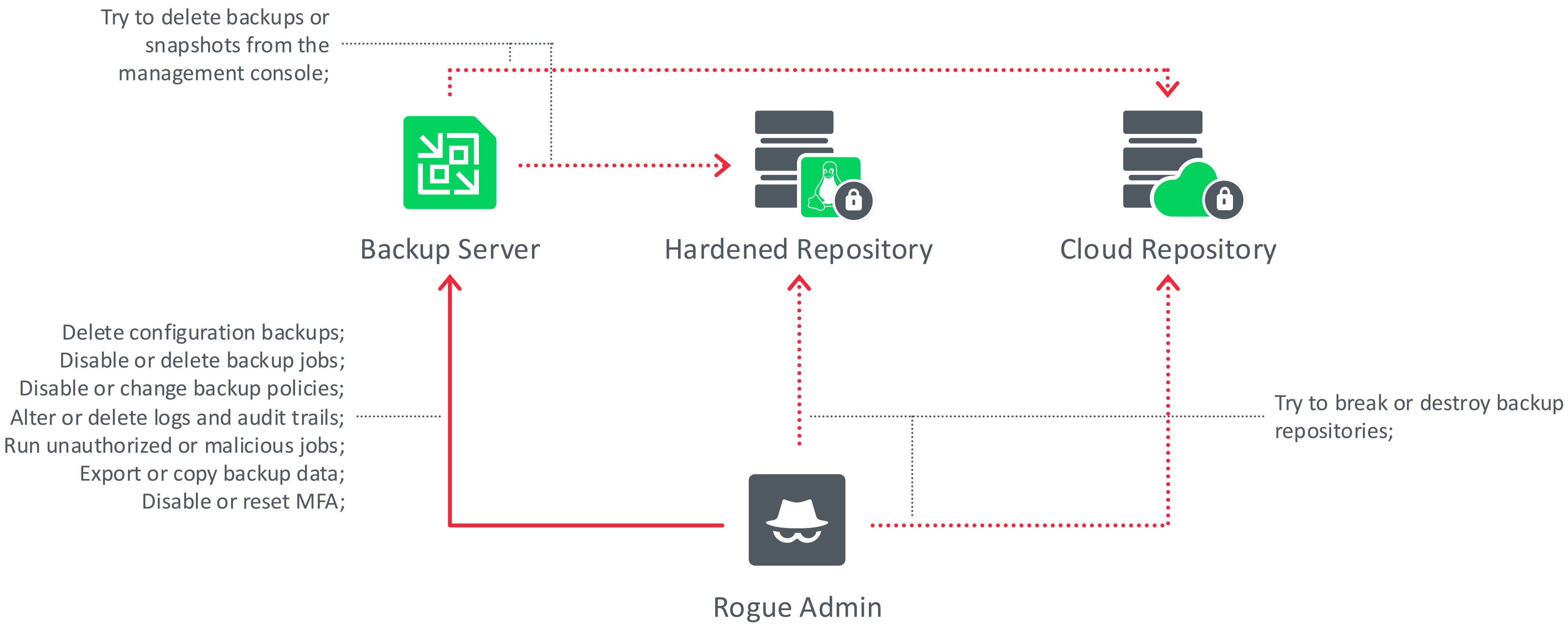
Some of these tools are open-source and community created, and some are from well-known security companies. Again, Google/AI to the aid.

Risk #4

Insider Threats

Statistics: authentication-based attacks and insider threats are increasing, with privileged users having elevated access to critical backup infrastructure.

Insider Threats

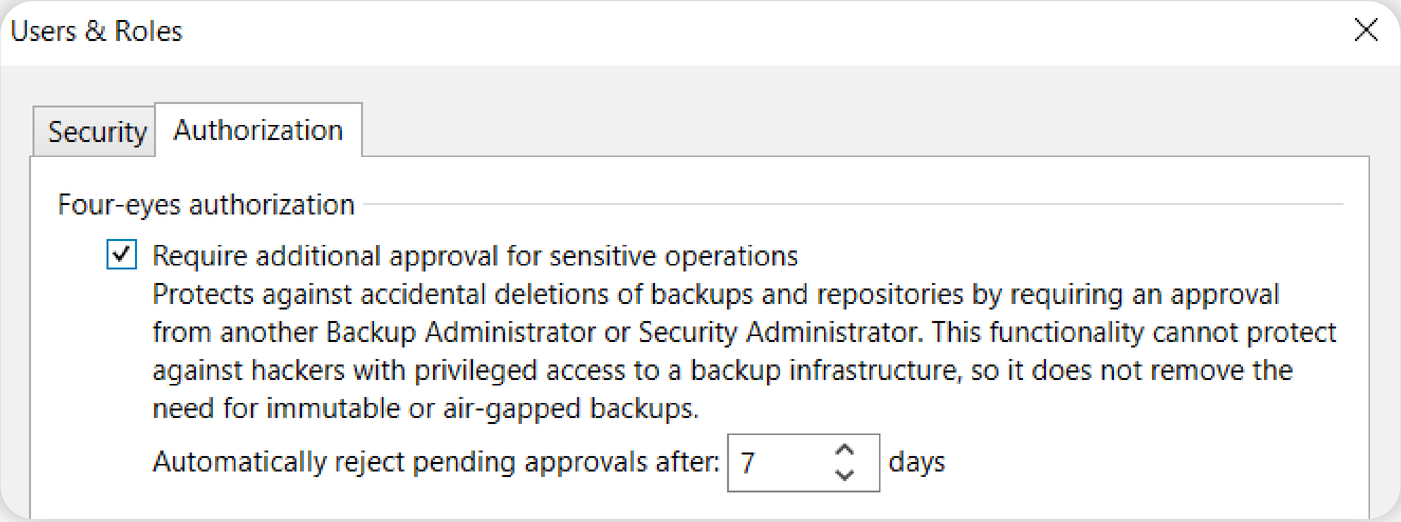

Try to delete backups or snapshots from the management console;
Backup Server
Hardened Repository
Cloud Repository
Delete configuration backups;
Disable or delete backup jobs;
Disable or change backup policies;
Alter or delete logs and audit trails;
Run unauthorized or malicious jobs;
Export or copy backup data;
Disable or reset MFA;
Try to break or destroy backup repositories;
Rogue Admin

Insider Threats

Four-Eyes Authorization

When enabled, four-eyes authorization is required for:

- Deleting backups, snapshots or configuration database
- Modifying or removing backup repositories and storage
- Managing users, groups and MFA settings
- Enabling or changing automatic logoff policies



Four-eyes authorization

☑ Require additional approval for sensitive operations

Protects against accidental deletions of backups and repositories by requiring an approval from another Backup Administrator or Security Administrator. This functionality cannot protect against hackers with privileged access to a backup infrastructure, so it does not remove the need for immutable or air-gapped backups.

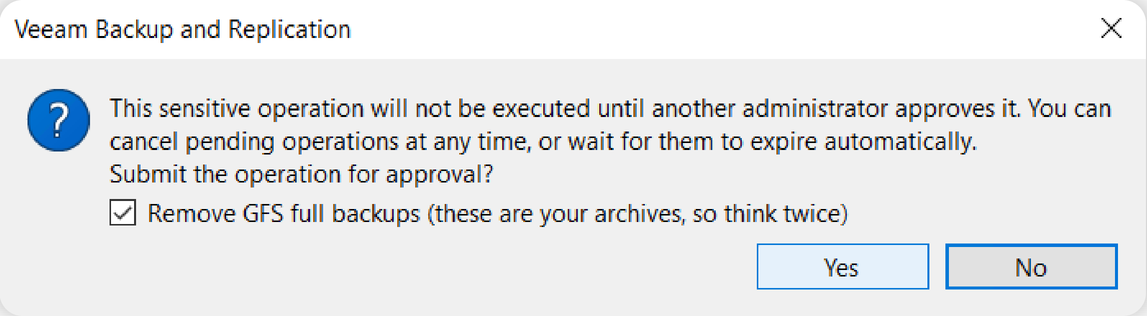
Automatically reject pending approvals after: 7 days

Insider Threats

Four-Eyes Authorization

Veeam Backup & Replication supports four-eyes authorization:

- When an admin tries to delete backup data or remove a repository, an approval request appears under Pending Approvals
- Specified recipients also receive an email notification


Veeam Backup and Replication

This sensitive operation will not be executed until another administrator approves it. You can cancel pending operations at any time, or wait for them to expire automatically.
Submit the operation for approval?

☑ Remove GFS full backups (these are your archives, so think twice)

Insider Threats

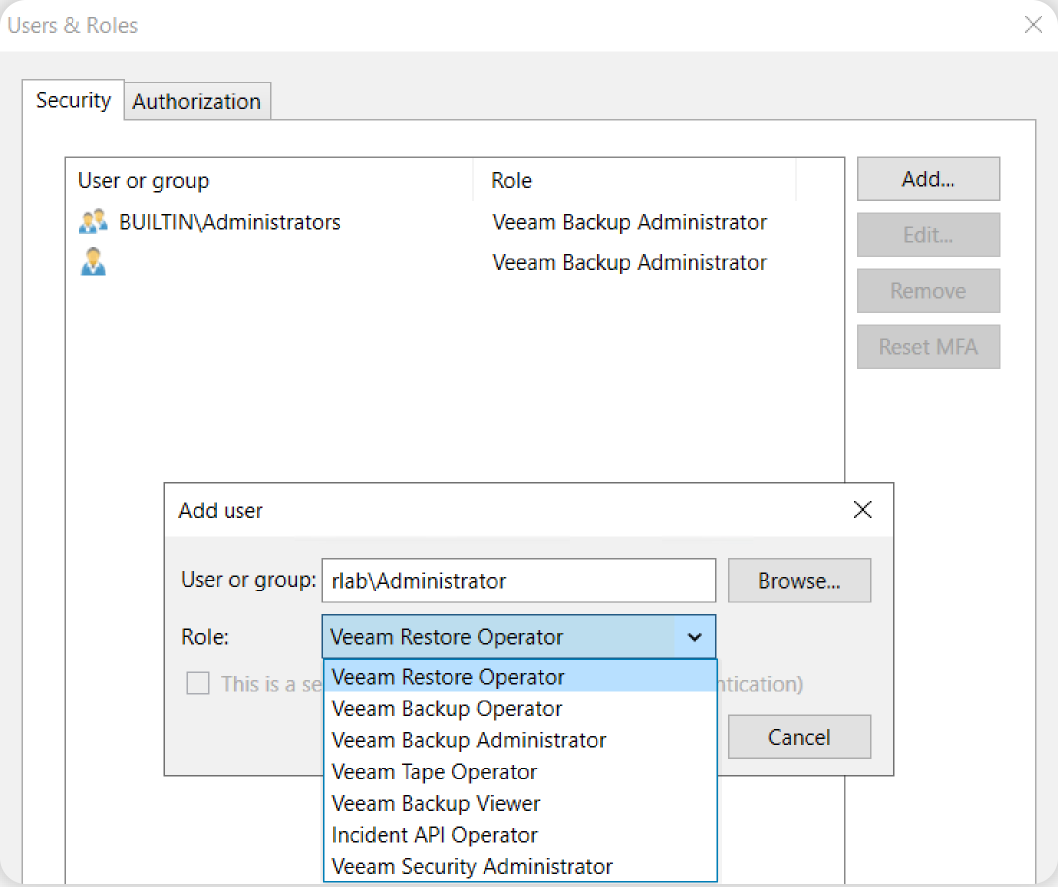
Use minimal necessary permissions

Use roles with minimal permissions necessary to perform the task

Reduces the risk of unauthorized access and data breaches

Minimizes attack surface by restricting user permissions to only what is needed

Enhances overall system security and stability



Users & Roles

User or group	Role
BUILTIN\Administrators	Veeam Backup Administrator
	Veeam Backup Administrator

Add user

User or group: rlab\Administrator

Role: Veeam Restore Operator

□ This is a se ntication)

Insider Threats

Security Officer

Approves requests for access elevation and other sensitive operations. However, the Security Officer cannot initiate the request.

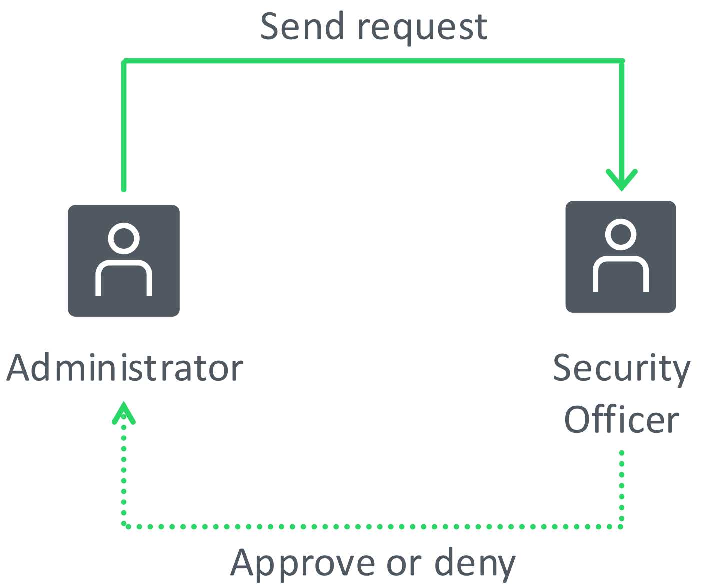
Root access for admin and password reset

Configuration backup restore

Enables advanced deployment options:

- High Availability
- Lockdown Mode
- Agent deployment for data collection

MFA settings change



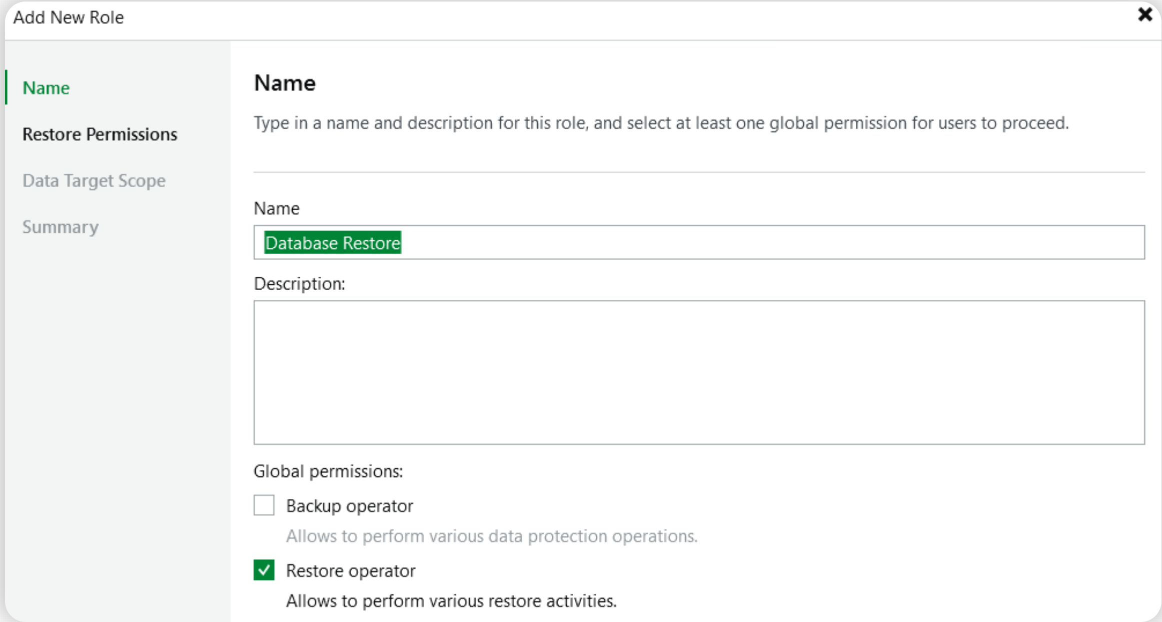
Insider Threats

Advanced RBAC

Advanced RBAC enables you to grant users access exclusively to specific scopes within both the backup infrastructure and the production environment.

Create custom roles to control access to:

- Backup and/or restore operations
- Repository
- Restore options
- Infrastructure objects



Add New Role

Name

Type in a name and description for this role, and select at least one global permission for users to proceed.

Name: Database Restore

Description:

Global permissions:

□ Backup operator
Allows to perform various data protection operations.

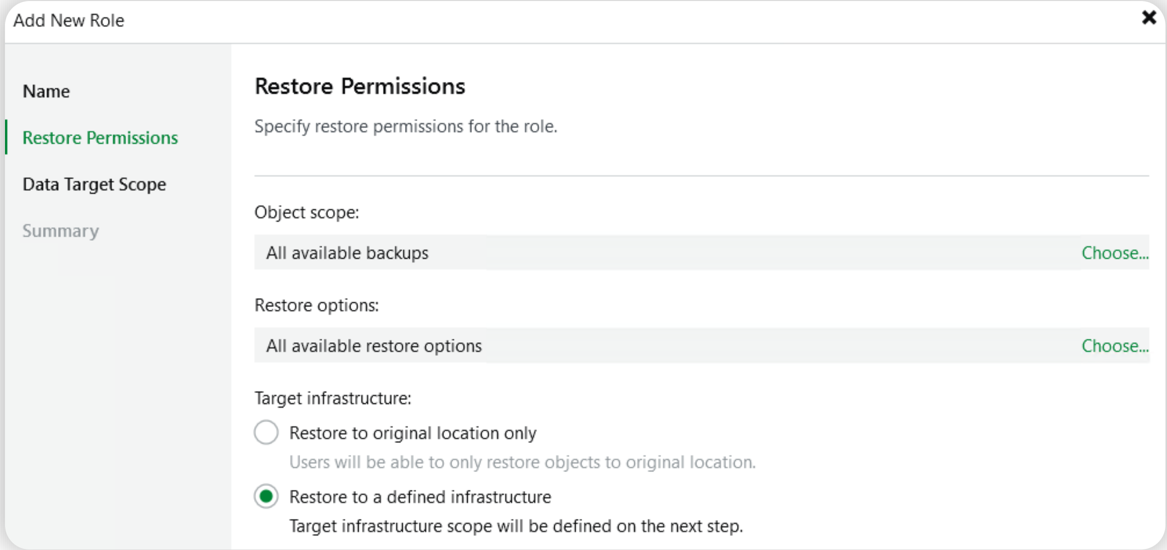
☑ Restore operator
Allows to perform various restore activities.

Insider Threats

Advanced RBAC

This precise permission control allows users to perform tasks such as backup or restoration without having unnecessary access to other parts of the infrastructure, improving security and reducing the risk of unauthorized actions.

Simply follow the principle of granting the minimum necessary access.



Add New Role

Restore Permissions

Specify restore permissions for the role.

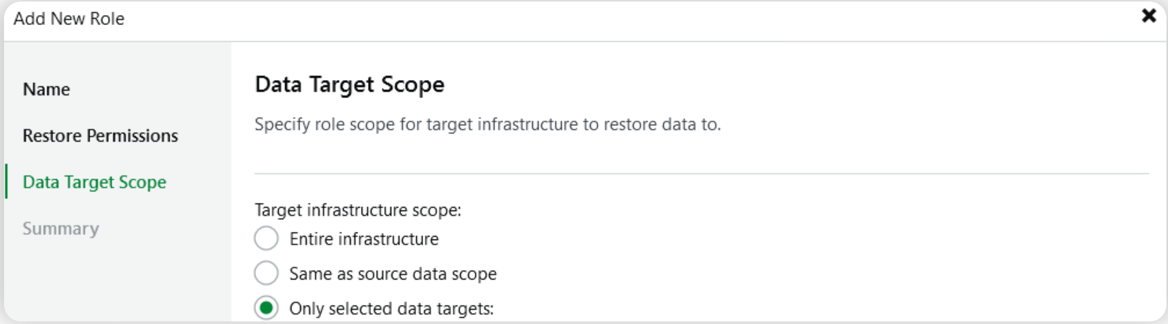
Object scope: All available backups

Restore options: All available restore options

Target infrastructure:

○ Restore to original location only
Users will be able to only restore objects to original location.

● Restore to a defined infrastructure
Target infrastructure scope will be defined on the next step.



Add New Role

Data Target Scope

Specify role scope for target infrastructure to restore data to.

Target infrastructure scope:

○ Entire infrastructure
○ Same as source data scope
● Only selected data targets:

Insider Threats

Monitoring: Veeam ONE for audit

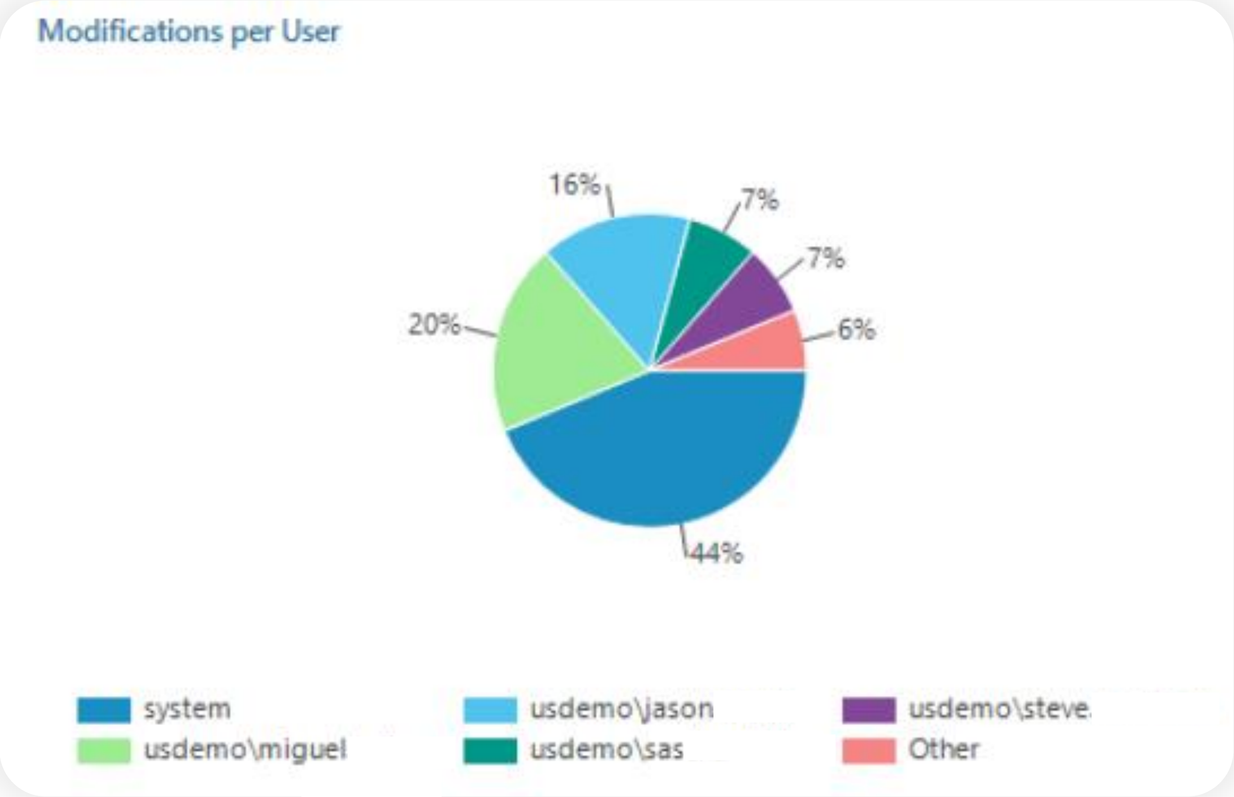
Audit information on all types of restores for accountability.

Detailed logs of job configuration changes, including timestamps and user accounts.

Tracks configuration changes in virtual environments with user-level details.

Monitors access and permission modifications for security compliance.

Generates comprehensive audit reports for regulatory and operational transparency.



Insider Threats

Do you have an immutable backup?

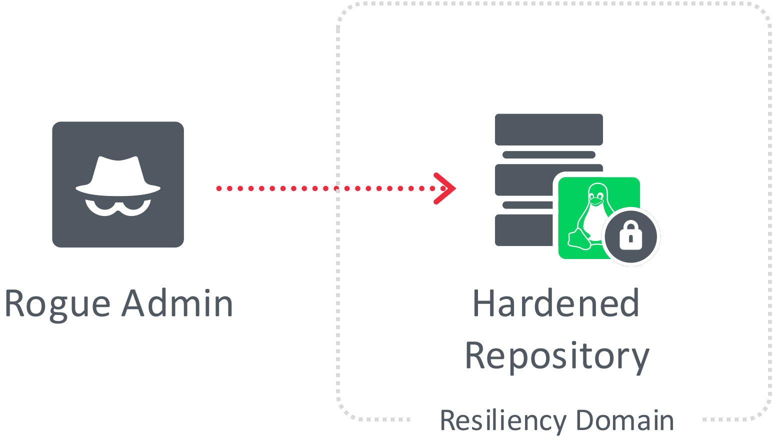
Single-use Linux credentials, not stored in Veeam database

Veeam services control data traffic ports (virtual airgap)

SSH is disabled and not required for Veeam upgrades

Prevents unauthorized modification or deletion of backups

Limits insider threats by restricting the ability to alter or erase stored data



Risk #5

Network-Based Lateral Movement

Statistics: median dwell time is 26 days when externally notified, but only 5 days in ransomware cases where attackers notify victims.

Network-Based Lateral Movement

What does it mean? How is that related to Veeam?

Attackers rarely stop at the system they first compromise. Instead, they map the environment, target additional systems, and adjust tactics depending on security controls encountered.

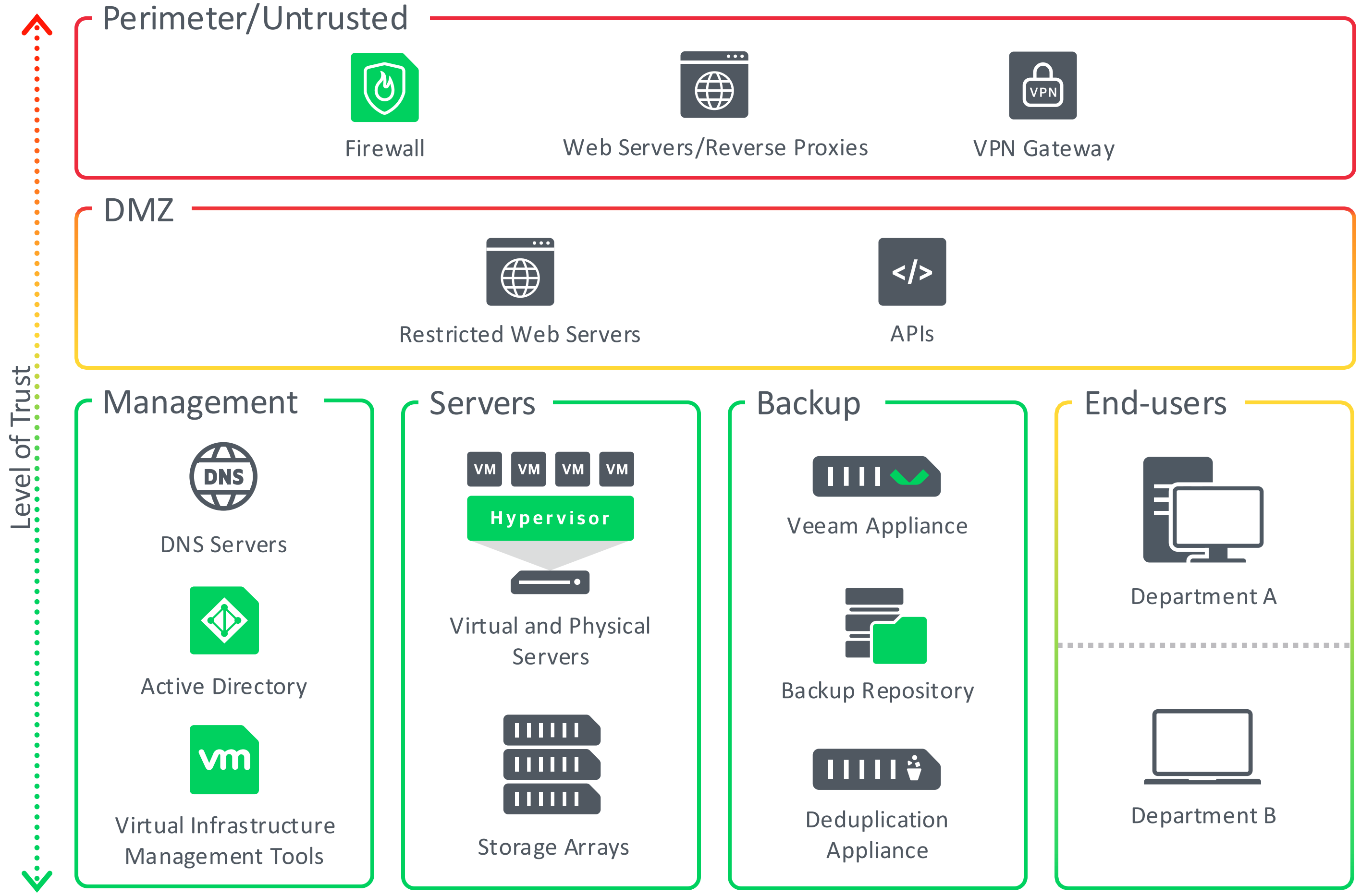
Lateral movement can utilize legitimate tools (PowerShell and BASH scripts, WMI, RDP, SSH, Nmap, SCP, Network shares, etc.) to blend in with normal activity, making it especially challenging to detect.

Attackers exploit network security weaknesses (e.g., poor segmentation, broad permissions, domain-joined backup servers) to move laterally and compromise additional systems.

As you already know, backup infrastructure is a high-value target for lateral movement because attackers want to sabotage disaster recovery capabilities.

Network-Based Lateral Movement

Network Segmentation: the example of zones



Limits Lateral Movement

Only necessary communications are allowed. Attackers can't easily jump from compromised to critical systems.

Synergises Perfectly

Combine with active threat detection like XDR/EDR, honeypots to lure attackers, and SIEM to be aware.

Compliance Enabler

Segmented architectures support legal, and regulatory obligations – protecting the organization both operationally and legally.

Network-Based Lateral Movement

What else besides Network Segmentation?

Encrypted Communications

Veeam encrypts management connections with self-signed TLS certificates by default. However, it is possible to use a certificate signed by an internal Certificate Authority for better controls.

Backup Infrastructure Hardening

MFA, Key Management System, Four-Eyes, RBAC (the new one is really granular), don’t join the AD domain, etc.

Monitoring

Veeam B&R/ONE generating real-time alerts for issues like backup failures, job anomalies, or unusual spikes in activity that can signal ransomware or infrastructure compromise and feeding these alerts directly to SIEM. SIEM can cross-reference with security trends/anomalies elsewhere on your network, quickly highlighting when your backup environment is at risk.

VBR Security Best Practices: Hardening

Guide to SIEM (Security Information & Event Management)

Network-Based Lateral Movement

Don’t stop fighting Shadow IT!

Expands attack surfaces

Unauthorized apps, cloud platforms, or remote access tools create hidden pathways that attackers can exploit. These pathways often evade standard network controls and monitoring.

Credential leakage and bridging

Users might save or share passwords via unsanctioned channels (like email, chat apps, or personal file stores), giving attackers footholds for credential-based lateral movement across segments.

Facilitates stealthy lateral movement

Attackers may use shadow IT tools for staging data, relaying commands, or transferring malware – blending in with regular traffic and making detection through conventional means much harder.

Reduces monitoring and actionable insight

It’s more difficult for traditional SIEMs and backup monitoring to detect lateral movement that leverages shadow IT since logs and traffic may not pass through approved or instrumented channels.

Risk #6

Data Poisoning

Statistics: data poisoning attacks represent a sophisticated threat where cybercriminals subtly alter data before backup operations, making backups unreliable for recovery purposes.

Data Poisoning

What is Data Poisoning?

Data poisoning in backups refers to a sophisticated cyberattack where attackers subtly alter or corrupt the original data before it is backed up. These malicious modifications, often unnoticed for long periods, make backup copies unreliable or compromised, undermining the entire recovery strategy.

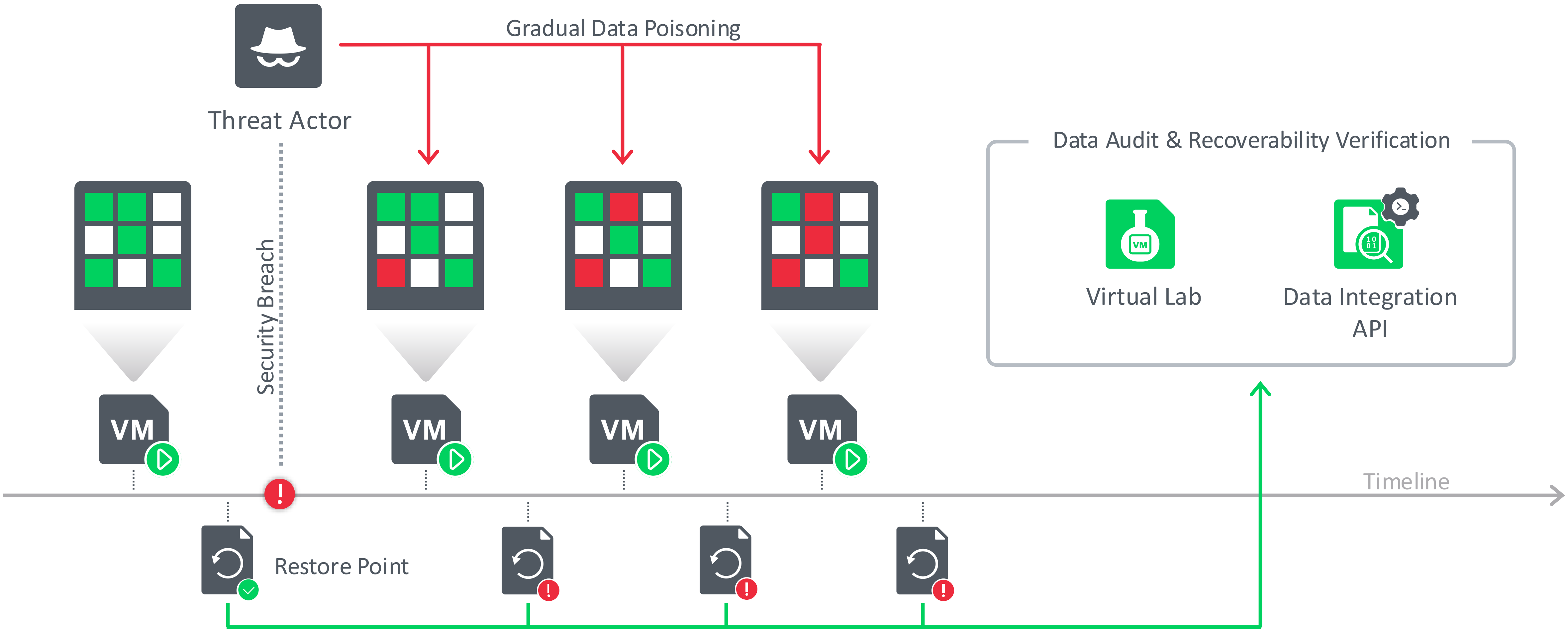
The changes are made in a way that looks just like normal mistakes or routine updates. Over weeks, months or even years, these little changes add up. Eventually, the data is so corrupted that it causes problems – such as financial losses, fake statistics, or mistakes in reports and decisions.

Unlike traditional ransomware or destructive attacks, data poisoning targets the validity and integrity of data itself, ensuring that even restored files are corrupted or hold invalid/altered data.

Such attacks often go unnoticed until data is validated or attempted recovery, causing costly downtime and data loss.

Data Poisoning

Gradual or “Low and Slow”



Data Poisoning

Clean Room Data Recovery: Enhancing Security and Data Integrity

Virtual Lab and Data Integration API

The Virtual Lab is a “clean room” or “sandboxed” environment that allows SureBackup jobs to test your backups without impacting production systems. This environment allows you to repeatedly test backups for both *recoverability* and *content integrity*.

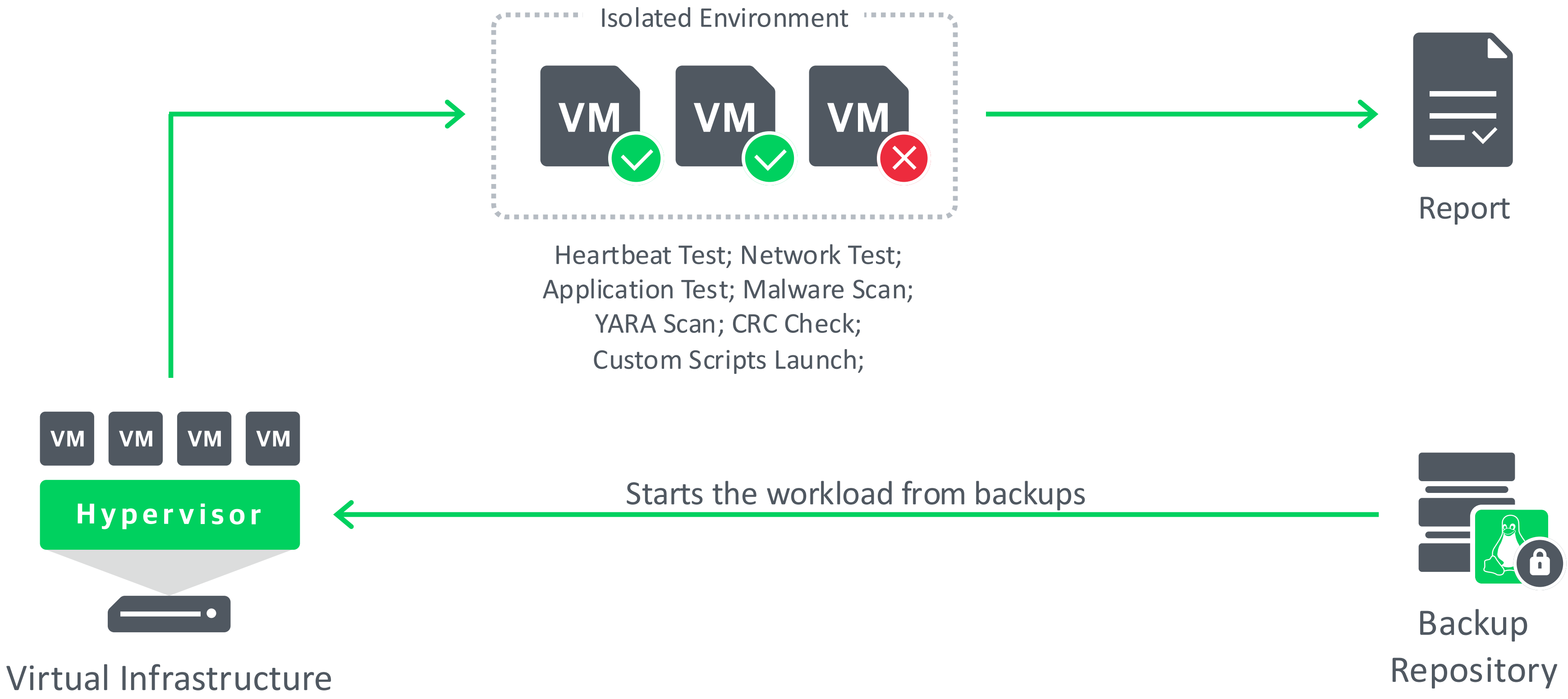
SureBackup verifies that critical services - such as databases, Active Directory, and email systems - function correctly within the sandbox. Any unusual application behavior during these tests may indicate stealthy forms of data poisoning.

The Data Integration API enables mounting backup data without full restoration, allowing you to run custom scripts, data mining, classification, analytics or forensic tools against backup data as part of automated workflows.

You can compare recent backups with trusted clean backups to detect data drift or unauthorized modifications. Suspicious or altered datasets can be exported for detailed human analysis or bulk reporting.

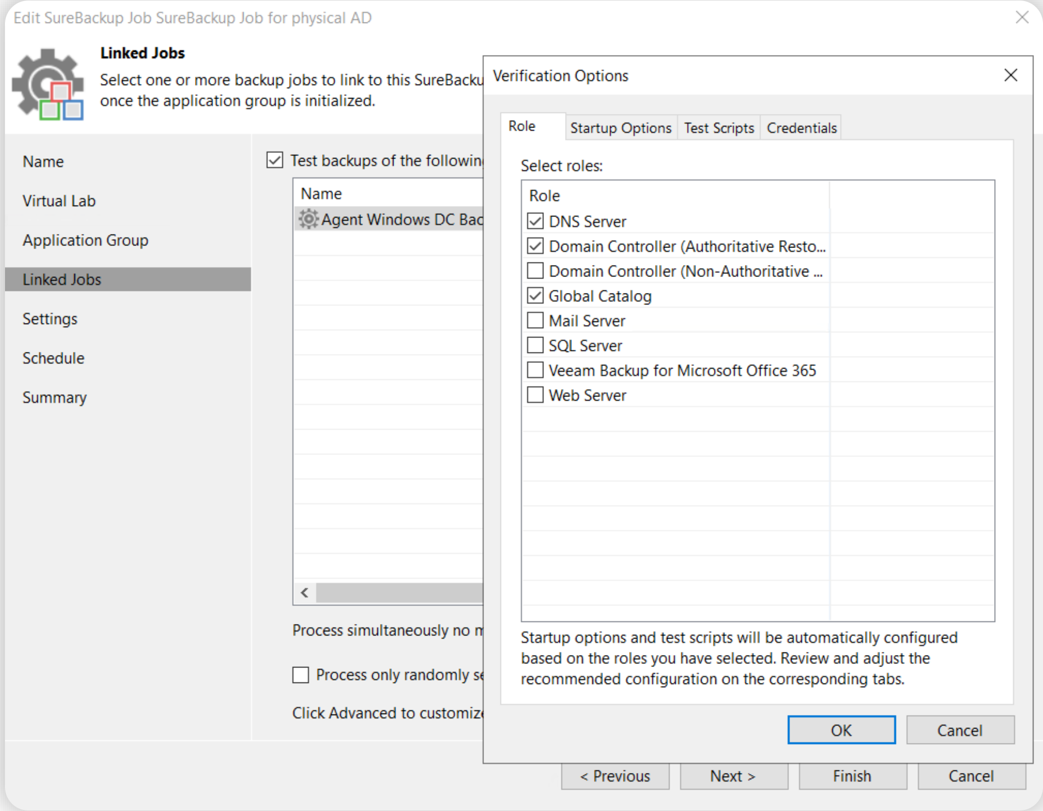
Data Poisoning

SureBackup Workflow



Data Poisoning

SureBackup



Edit SureBackup Job SureBackup Job for physical AD

Linked Jobs

Select one or more backup jobs to link to this SureBacku
once the application group is initialized.

- Name
- Virtual Lab
- Application Group
- Linked Jobs
- Settings
- Schedule
- Summary

☑ Test backups of the followin

Name
Agent Windows DC Bac

Process simultaneously no m

☐ Process only randomly se

Click Advanced to customiz

< Previous | Next > | Finish | Cancel

Verification Options

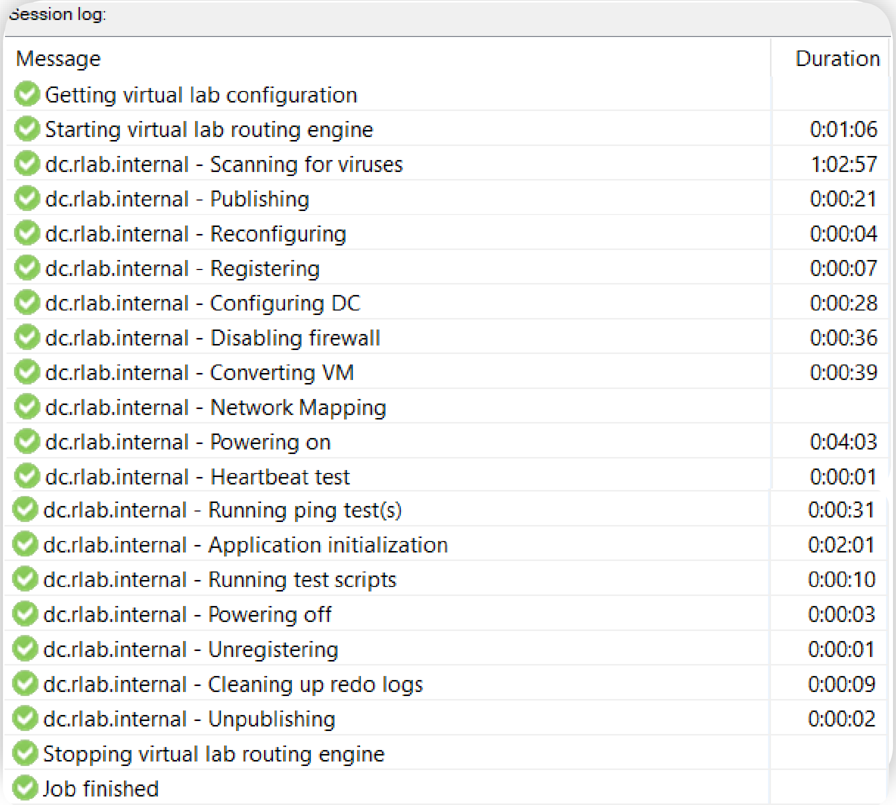
Role | Startup Options | Test Scripts | Credentials

Select roles:

Role
☑ DNS Server
☑ Domain Controller (Authoritative Resto...
☐ Domain Controller (Non-Authoritative ...
☑ Global Catalog
☐ Mail Server
☐ SQL Server
☐ Veeam Backup for Microsoft Office 365
☐ Web Server

Startup options and test scripts will be automatically configured based on the roles you have selected. Review and adjust the recommended configuration on the corresponding tabs.

OK | Cancel

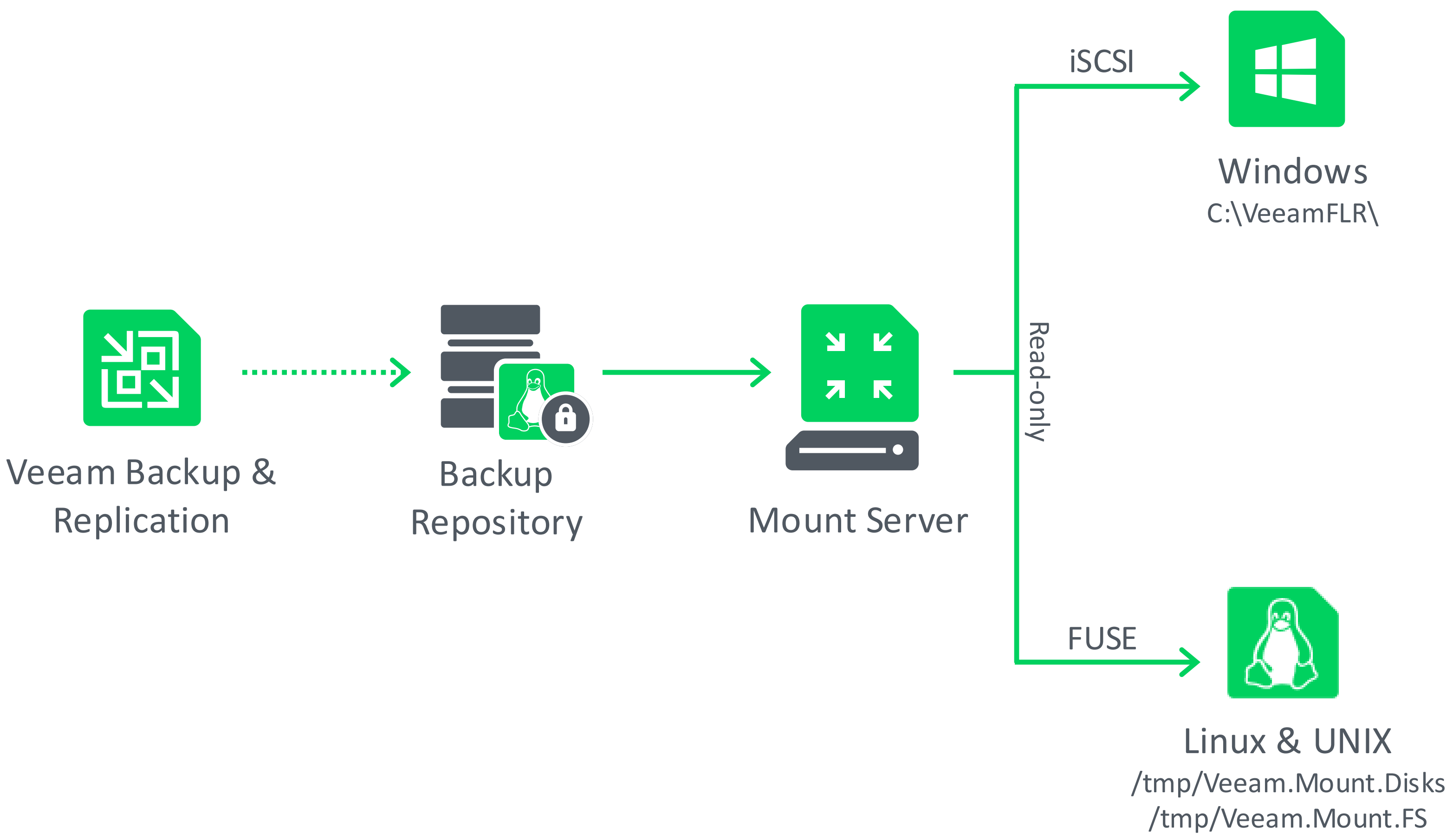


Session log:

Message	Duration
✓ Getting virtual lab configuration	
✓ Starting virtual lab routing engine	0:01:06
✓ dc.rlab.internal - Scanning for viruses	1:02:57
✓ dc.rlab.internal - Publishing	0:00:21
✓ dc.rlab.internal - Reconfiguring	0:00:04
✓ dc.rlab.internal - Registering	0:00:07
✓ dc.rlab.internal - Configuring DC	0:00:28
✓ dc.rlab.internal - Disabling firewall	0:00:36
✓ dc.rlab.internal - Converting VM	0:00:39
✓ dc.rlab.internal - Network Mapping	
✓ dc.rlab.internal - Powering on	0:04:03
✓ dc.rlab.internal - Heartbeat test	0:00:01
✓ dc.rlab.internal - Running ping test(s)	0:00:31
✓ dc.rlab.internal - Application initialization	0:02:01
✓ dc.rlab.internal - Running test scripts	0:00:10
✓ dc.rlab.internal - Powering off	0:00:03
✓ dc.rlab.internal - Unregistering	0:00:01
✓ dc.rlab.internal - Cleaning up redo logs	0:00:09
✓ dc.rlab.internal - Unpublishing	0:00:02
✓ Stopping virtual lab routing engine	
✓ Job finished	

Data Poisoning

Data Integration API Workflow



Use Cases

- Data mining
- Classification
- Analytics
- Forensic tools
- Security Analysis
- Malware Scanning
- eDiscovery
- GDPR Auditing
- ML Applications
- Data Comparison
- Integrity Checking

Data Poisoning

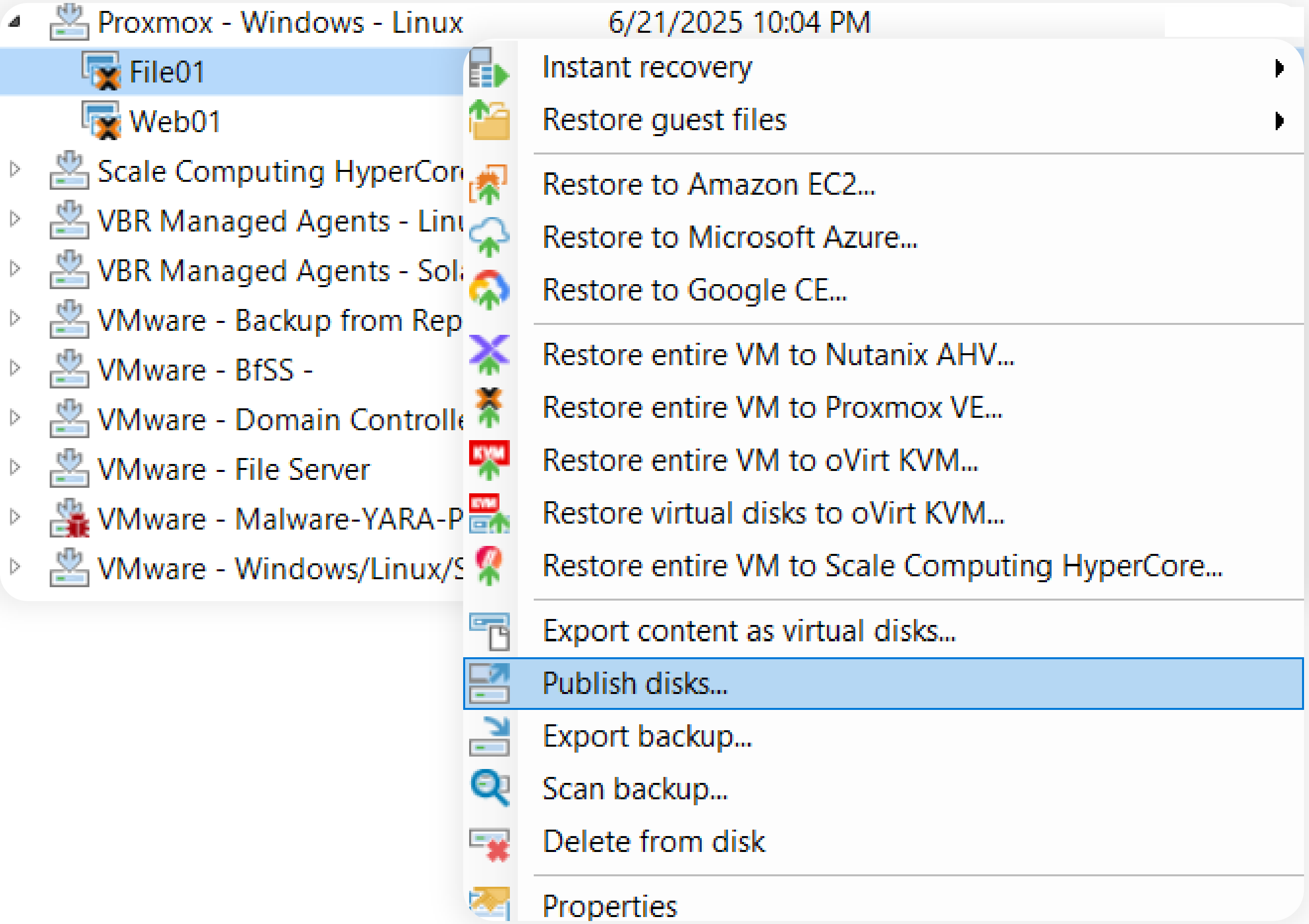
Data Integration API

The Data Integration API (REST) is the programmatic version of Publish disks…

It enables automation, integration, and repeatable workflows.

Effectively it’s the “backend” that the Publish disks… uses under the hood.

It’s possible to use PowerShell scripts to automate Publish disks… as well.



Proxmox - Windows - Linux
6/21/2025 10:04 PM
File01
Web01
Scale Computing HyperCor
VBR Managed Agents - Linu
VBR Managed Agents - Sola
VMware - Backup from Rep
VMware - BfSS -
VMware - Domain Controlle
VMware - File Server
VMware - Malware-YARA-P
VMware - Windows/Linux/S
Instant recovery
Restore guest files
Restore to Amazon EC2...
Restore to Microsoft Azure...
Restore to Google CE...
Restore entire VM to Nutanix AHV...
Restore entire VM to Proxmox VE...
Restore entire VM to oVirt KVM...
Restore virtual disks to oVirt KVM...
Restore entire VM to Scale Computing HyperCore...
Export content as virtual disks...
Publish disks...
Export backup...
Scan backup...
Delete from disk
Properties

Risk #7

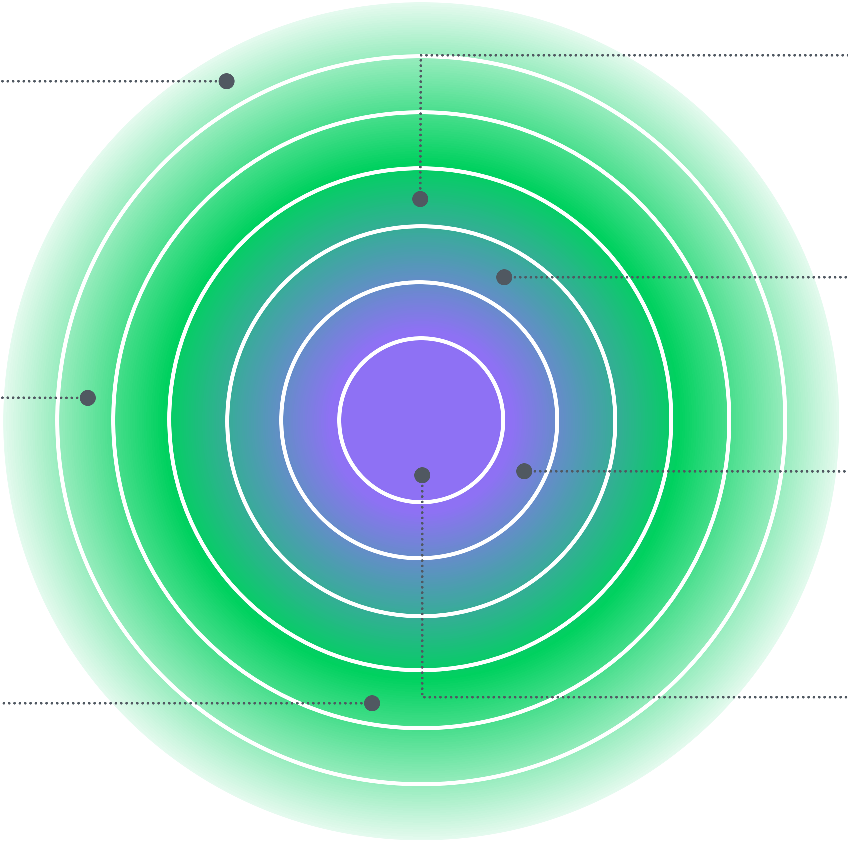
General Environment Vulnerabilities

Many organizations lack proper security configurations despite having playbooks and best practices.

A chain is only as strong as its weakest link…

General Environment Vulnerabilities

Security Layers



Human Layer

Most breaches exploit human error—phishing, social engineering, weak passwords.

Perimeter Security Layer

This is the "outer fence" – where you deter or block external attackers.

Network Security Layer

Prevents lateral movement and limits the spread of threats inside your environment.

Endpoint Security Layer

Every device (PC, server, mobile) is a potential entry point.

Application Security Layer

Applications are frequent targets for exploitation.

Data Security Layer

The real target is your data – whether theft, ransom, or sabotage.

Mission-Critical Assets Layer

Systems/data essential for business continuity require special safeguards.

General Environment Vulnerabilities

It's not just about VDP configuration

Imagine, you're configuring a new server…

1. Would you change the default credentials?
2. Would you configure the logging to external monitoring system?
3. Are you going to update all the firmware and do it regularly?
4. Would you ensure that its management interfaces are added to the isolated 'management' network segment?
5. Would you disable unused physical ports and Interfaces?
6. Would you disable legacy management/auth protocols (Telnet/NTLM/SNMPv1/HTTP) and leave only the most secure (SSH/HTTPS)?
7. Would you follow the hardening baseline (DISA STIG, NIS2, etc.) when configuring the rest?

General Environment Vulnerabilities

It's not just about VDP configuration

Think about your environment in general…

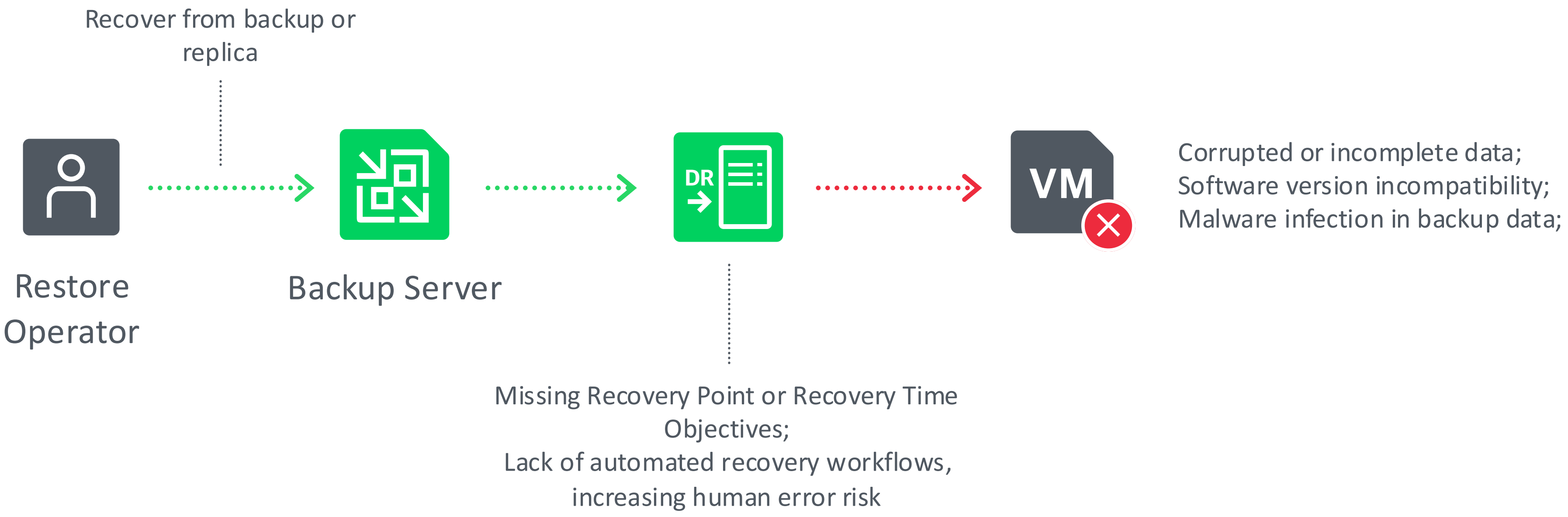
1. When was the last time you reviewed the list of admins for dormant/ghost?
2. How many of active firewall configuration rules allowing more than they should do you have? Just look for ‘allow any’.
3. Have you ever run a port scanner from untrusted/semi-trusted networks?
4. Do you use any operating systems that are in an end-of-life state?
5. How long ago did you simulate a security event (invalid login, privilege escalation) to ensure it was logged by SIEM?
6. Have you ever had a security training for the employees of your organisation? What about simulated phishing/social engineering to test real-world user behaviour?
7. Wi-Fi, physical security, endpoint hardening, cloud(s)…

Risk #8

Recovery and Orchestration Failures

Disaster recovery and recovery orchestration failures are often caused by insufficient testing, outdated recovery plans and a lack of documentation or automation.

Recovery and Orchestration Failures



Recover from backup or replica

Restore Operator

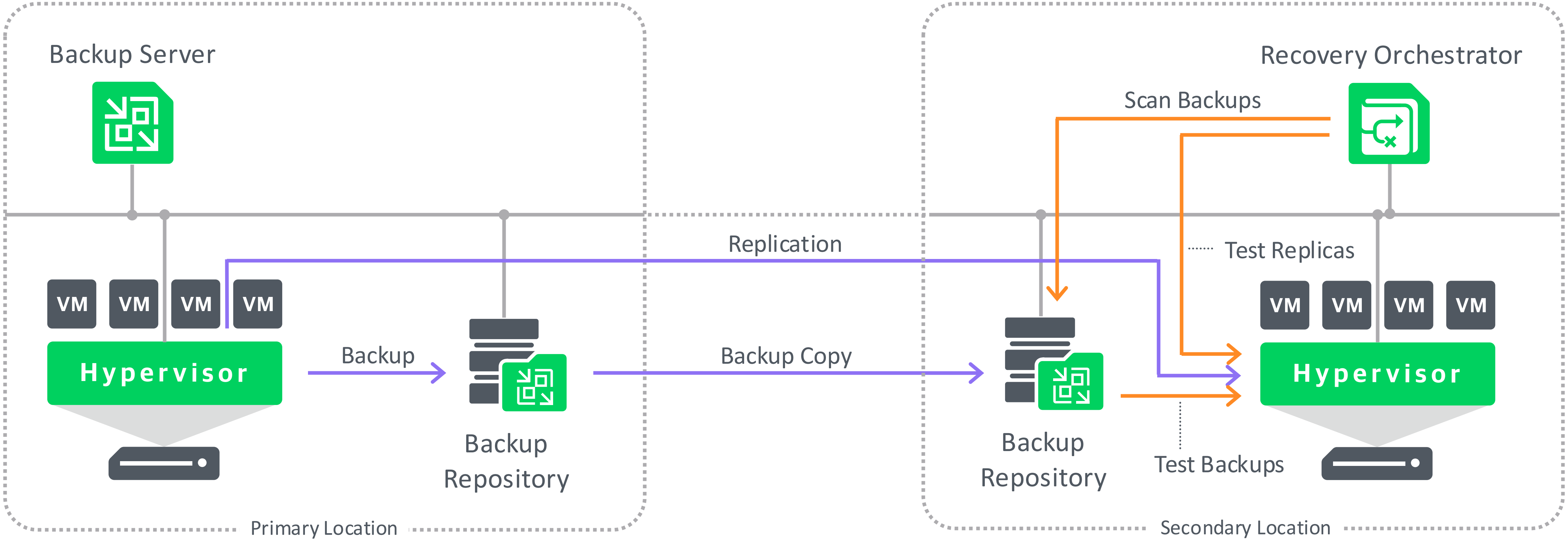
Backup Server

Corrupted or incomplete data;
Software version incompatibility;
Malware infection in backup data;

Missing Recovery Point or Recovery Time Objectives;
Lack of automated recovery workflows, increasing human error risk

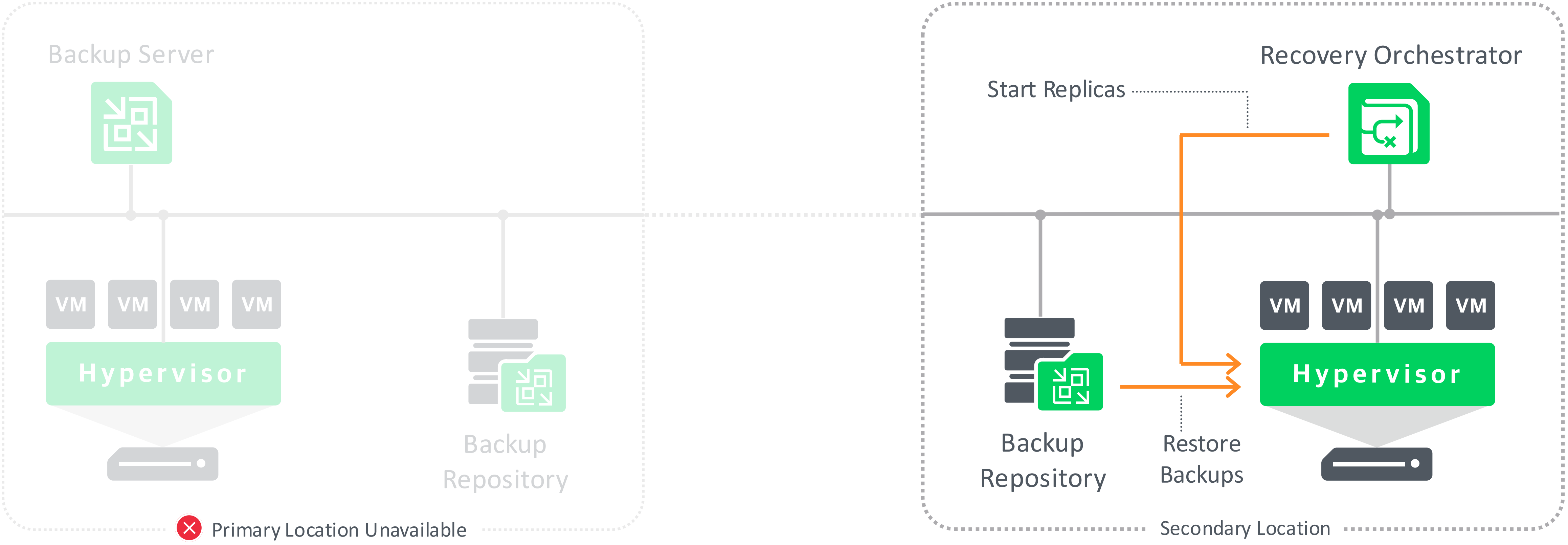
Recovery and Orchestration Failures

Regular Operations



Recovery and Orchestration Failures

Failover



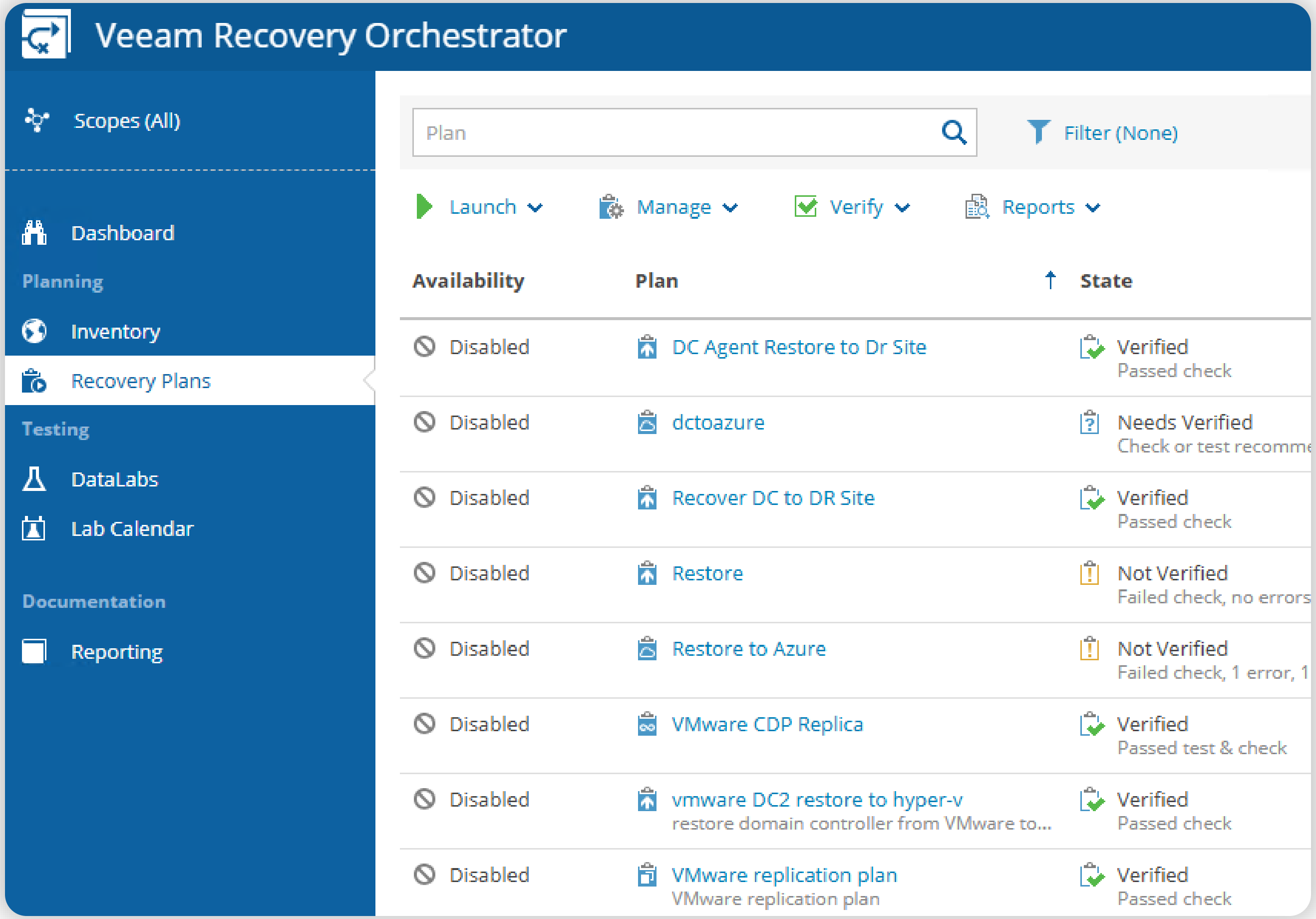
Recovery and Orchestration Failures

Create Plan

Define recovery objectives including RTO and RPO to align with business requirements

Map out critical applications, dependencies, and infrastructure components to ensure comprehensive recovery coverage

Include required validation steps for applications and services within the recovery plan



Availability	Plan	State
Disabled	DC Agent Restore to Dr Site	Verified Passed check
Disabled	dctoazure	Needs Verified Check or test recomme
Disabled	Recover DC to DR Site	Verified Passed check
Disabled	Restore	Not Verified Failed check, no errors
Disabled	Restore to Azure	Not Verified Failed check, 1 error, 1
Disabled	VMware CDP Replica	Verified Passed test & check
Disabled	vmware DC2 restore to hyper-v restore domain controller from VMware to...	Verified Passed check
Disabled	VMware replication plan VMware replication plan	Verified Passed check

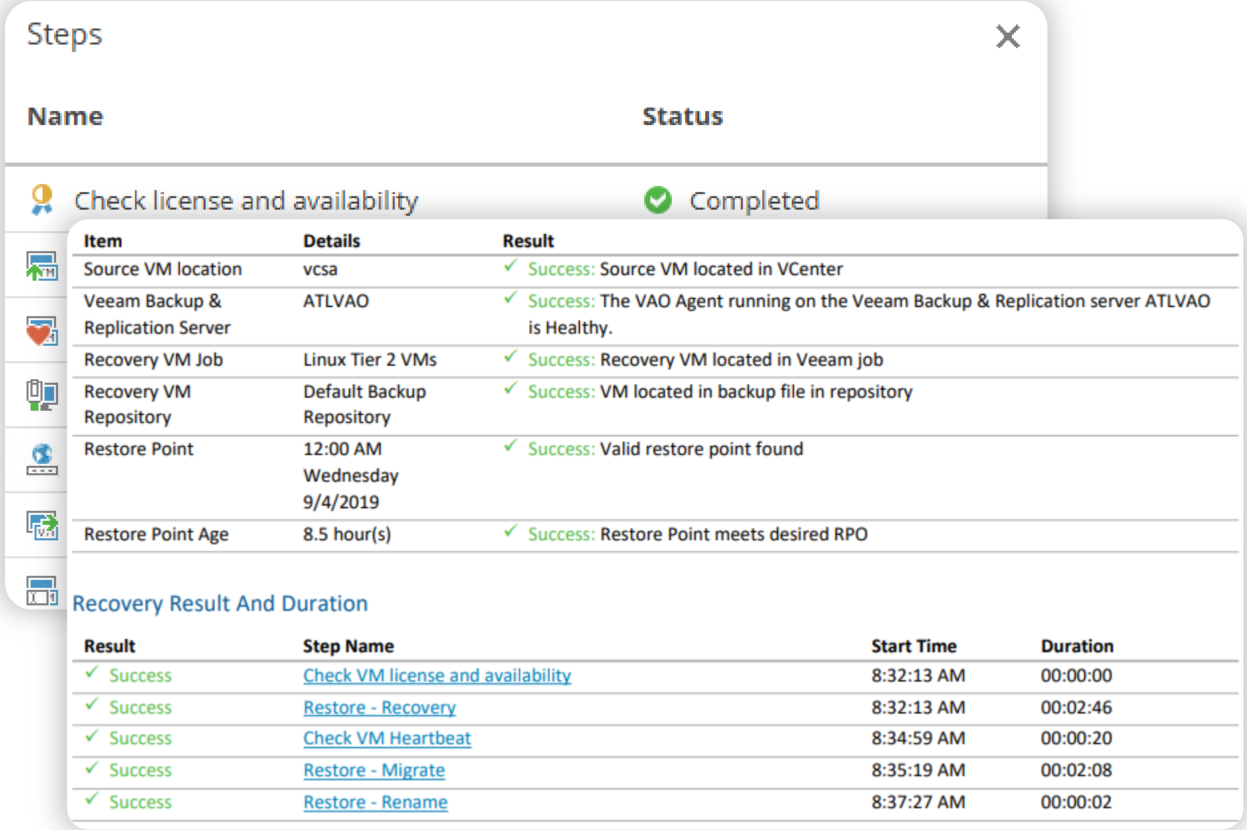
Recovery and Orchestration Failures

Validate and Test

Perform automated recovery verification tests in isolated environments to ensure backups are recoverable without impacting production

Generate detailed validation reports highlighting success rates, potential issues, and areas for improvement.

Conduct regular, scheduled validation exercises to maintain compliance and readiness for actual disaster recovery scenarios.



Steps

Name	Status
Check license and availability	✓ Completed

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

Discover More Useful Resources

Veeam Backup & Replication Security Best Practice Guide

Veeam Security Knowledge Base Article List

Ransomware Trends and Proactive Strategies Report 2025

Veeam Cyber Secure Program

Veeam University Free

Veeam University Pro

Veeam Hands-On Labs

Follow us!

Join the community hub: