Veeam Data Platform

First 100 Days

A Practical Onboarding Guide for IT Administrators

Contents

1. Executive Summary

Veeam Data Platform is your organization's foundation for ransomware resilience and operational continuity. This guide is designed to help IT teams operationalize and mature their environment in a structured manner. Although we use the term "first 100 days", that is just a metaphor for a timeline. Every organization is different and may progress at varying speeds, but the goal is the same: Moving from initial setup toward a more secure, resilient, and recovery-ready state. It is structured around practical milestones and recommended outcomes rather than strict implementation requirements, allowing you to focus on the steps most relevant to your environment and edition.

2. Who Is This Guide For?

This guide is for **IT administrators** who are deploying, configuring, and operationalizing Veeam Data Platform. It assumes you have familiarity with virtualized infrastructure (e.g., VMware vSphere, Microsoft Hyper-V, or any other hypervisor supported by Veeam Backup & Replication) and basic Windows Server administration. No Linux expertise is required.

It also serves as a shared reference for **IT managers** who are tracking scope and timelines, security and compliance stakeholders who are validating hardening posture, and leadership or procurement teams by defining what Day 100 success looks like.

3. What You Will Achieve by Day 100

By Day 100, you will have a stable, hardened, and verifiably recoverable environment that reduces outage risk and enables fast, confident recovery no matter what.

Every customer should be able to confirm the following checkpoints are met:

- **Deployed:** Veeam Backup & Replication is running, connected, and sized to meet backup windows.
- **Protected:** Priority workloads are backed up successfully on a defined schedule.
- **Hardened:** Immutability is in place locally and/or offsite to defend against ransomware.
- **Verifiably recoverable:** Restore testing is complete, documented, and mapped to recovery time objective and recovery point objective (RTO and RPO) targets.
- **Operationalized:** Monitoring, alerting, reporting, and recovery runbooks are in place and owned.

4. Roadmap at a Glance

This guide is structured into four sequential phases, each building toward Day 100 outcomes:

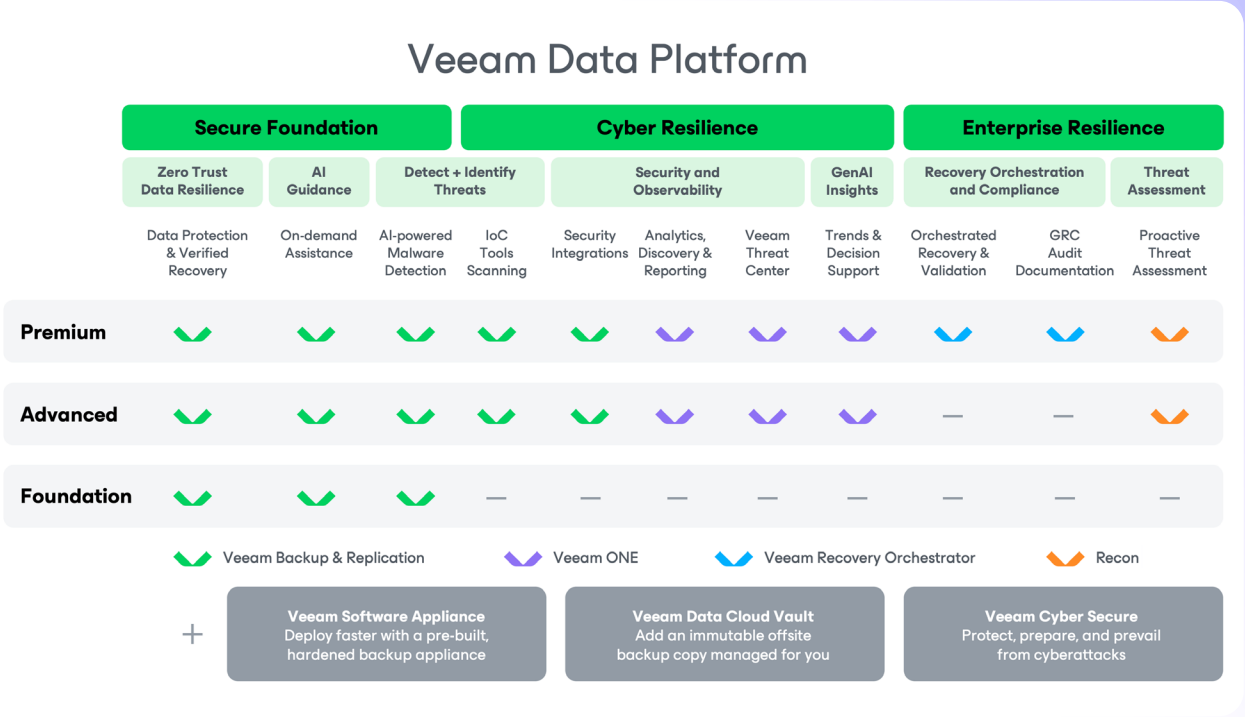
Phase	Name	Timeline	Focus
PHASE 1	Foundation	Days 1–14	Size environment, deploy Veeam Software Appliance (and Veeam Infrastructure Appliance if applicable), run first backup jobs, prepare for Veeam Recovery Orchestrator.
PHASE 2	Optimize	Days 15–45	Application-aware processing, backup copy jobs, Veeam Data Cloud Vault offsite tier, and Veeam Recovery Orchestrator setup (Premium).
PHASE 3	Data and Business Resilience	Days 46–75	Close coverage gaps, enable Recon, ransomware readiness, tuning, and build orchestration plans (Premium).
PHASE 4	Prove Value	Days 76–100	Orchestrated recovery testing, reporting, document architecture, and ongoing hygiene.

How to Use This Guide

- Follow the milestones in order. Skipping ahead, particularly to Scale-out Backup Repository (SOBR) configuration or Vault, before your local repositories and jobs are stable creates gaps that typically surface during a real restore.
- The timeline is flexible. Days are guidelines, not hard deadlines. Smaller environments may complete Phase 1 in under a week. More complex environments may require more time in later phases.
- Use the decision points. When architecture choices arise (for example, deployment path or repository strategy), pause, align stakeholders, and document your decision before proceeding.
- Skip what does not apply, but note why. If your edition does not include Veeam ONE or Veeam Recovery Orchestrator, those milestones will be clearly marked. Similarly, Veeam Software Appliance and Veeam Vault steps are optional and relevant only if those modules are part of your deployment.

Veeam Data Platform Overview

Before diving into deployment and how to do it, let's get started with a quick recap of what your Veeam Data Platform includes. Veeam Data Platform is available in three editions, each building on the last:



See the appendix for descriptions of all components: "Appendix: Quick Reference. Key Components".

Take a moment to confirm your edition.

Before moving forward, confirm your edition and take full inventory of what's included. In data protection, unused capabilities aren't just wasted value — they're gaps waiting to be exposed.

Additionally, the following modules are available across all editions:

- **Veeam Software Appliance:** A pre-hardened, Windows-free deployment platform that simplifies infrastructure setup and strengthens security posture. No Linux expertise is required.
- **Veeam Vault:** Immutable, off-site backup storage delivered as a service to protect your data against ransomware and accidental deletion.
- **Veeam Agents:** Veeam Agents are software agents that bring Veeam-grade image-level backup and recovery to physical servers, endpoints, and unsupported virtual machine (VM) platforms, managed centrally from the Veeam Backup & Replication console.

The Road to Resilience Starts Here

Over the next 100 days, you'll go from deployment to a fully hardened, verifiably recoverable environment milestone by milestone with no guesswork.

PHASE 1 **Foundation** **Days 1–14**	PHASE 2 **Optimize** **Days 15–45**	PHASE 3 **Data and Business Resilience** **Days 46–75**	PHASE 4 **Prove Value** **Days 76–100**
M1: Size and Plan	M4: App-Aware Processing	M7: Close Coverage Gaps	M10: Recovery Testing
M2: Deploy Veeam Software Appliance and Infrastructure	M5: Backup Copy, SOBR, and Vault	M8: Ransomware Readiness	M11: Reporting and Docs
M3: First Backup Jobs	M6: Monitoring, Alerting, and Orchestrator Setup	M9: Performance Tuning and Orchestration Plans	M12: Ongoing Hygiene

PHASE 1 • Days 1–14

Foundation

Goal: Infrastructure sized, deployed, and first workloads protected.

Milestone 1: Size and Plan

Before deploying anything, invest time in sizing. Undersized infrastructure is the most common cause of slow backup windows and missed RPOs in the first 100 days.

Workload Inventory

- Document your total VM and workload count, data footprint (total provisioned vs. used), and estimated daily change rate.
- Identify your most critical workloads, since these drive your RPO and RTO targets.
- Note any physical workloads (e.g., Windows/Linux servers) that will require Veeam Agents.

Veeam Software Appliance Sizing

- Veeam Software Appliance ships with Veeam Backup & Replication pre-installed, so your primary sizing decision is the host it runs on.
- Minimum for small-to medium-sized businesses (SMBs): 8 vCPU / 16 GB RAM (recommended 500 MB RAM for each concurrent job).
- Use the Veeam Sizing Calculator (calculator.veeam.com) to validate resource requirements for your workload count and data footprint.
- Choose your deployment form factor: An OVA for VMware vSphere or an ISO for physical servers and other hypervisors. No Linux experience is required either way.

Storage Architecture: Choose Your Path

Your storage choice at this stage shapes the rest of Phases 1 and 2. There are three recommended paths for SMB:

Path A: Veeam Software Appliance + Veeam Infrastructure Appliance as a Veeam Hardened Repository + Vault: This is the recommended baseline. This path provides a local immutable repository without requiring Linux expertise, plus off-site and logically air-gapped immutable copies via Vault.

Path A: Why use a Veeam Hardened Repository delivered via Veeam Infrastructure Appliance?

A Veeam Hardened Repository provides immutable local backups. This means ransomware cannot encrypt or delete them during the retention period.

Traditionally, an immutable Linux repository requires a dedicated Linux server and manual OS hardening. Veeam Infrastructure Appliance removes that barrier entirely. It ships pre-hardened, deploys from an OVA or ISO, and requires no Linux expertise to stand up or maintain.

Veeam Infrastructure Appliance is a single-role appliance. Each instance runs as either a Veeam Hardened Repository or a Backup Proxy. For SMBs without a dedicated Linux admin or existing immutable storage, a Veeam Infrastructure Appliance-delivered Veeam Hardened Repository is the recommended path to local immutability.

For maximum protection, deploy Veeam Infrastructure Appliance on physical hardware. Running Veeam Infrastructure Appliance as a virtual appliance still inherits the hypervisor's attack surface. File system-level immutability protects backup files from in-OS attacks, but a hypervisor admin can still delete VMs out from under the immutable files.

Path B: Veeam Software Appliance + Veeam Data Cloud Vault: Veeam Backup & Replication writes backups directly to the local repository on Veeam Software Appliance and maintains a copy offsite in Veeam Vault. This is ideal for micro-SMBs, branch offices, or customers who want to minimize local storage management, plus off-site and logically air-gapped immutable copies via Vault. Keep in mind, if Veeam Software Appliance is deployed on a virtual infrastructure, it is not an adequate substitute for onsite immutability.

Path B: Why Veeam Software Appliance + Vault?

Path B keeps storage administration minimal. Veeam Backup & Replication writes backups to a local repository on Veeam Software Appliance itself, then a backup copy job replicates them offsite to Vault.

Veeam Software Appliance's local storage is immutable by default, so Path B still gives you on-premises ransomware protection. It is not a formal Veeam Hardened Repository in the product sense, so Path A remains the most rock-solid choice when you have hardware to dedicate to Veeam Infrastructure Appliance, but Path B is the right call when you don't. As with Path A, Veeam Software Appliance running as a virtual appliance can still be deleted at the hypervisor layer, so deploy on physical hardware where possible.

Path B skips the Veeam Infrastructure Appliance step entirely. If you pick this path, proceed from Milestone 2 (Veeam Software Appliance deployment) directly to Milestone 5 (backup copy job to Vault).

Path C: Veeam Software Appliance + existing NAS/Windows repository + Vault or alternative third-party off-site storage: This path leverages existing storage infrastructure and is less hardened locally unless additional configuration is applied. This is useful for when customers want to leverage existing Veeam Cloud & Service Provider (VCSP) partners for off-site storage or alternative off-site storage they already have available.

Regardless of your path:

- Consider isolating backup traffic onto a dedicated VLAN or NIC to keep backup data off your production network.
- Review your socket/workload licensing coverage before deployment.

Milestone 2: Deploy Veeam Software Appliance and Infrastructure

Deploy Veeam Software Appliance

- Download Veeam Software Appliance OVA (for VMware vSphere) or ISO (for physical servers or VMs on other supported hypervisors) from the Veeam Customer Portal (my.veeam.com).
- For OVA: Import into VMware vSphere and power on. Veeam Backup & Replication will be accessible via the management interface after first boot.
- For ISO: Boot the target server (e.g., physical or a VM on any other supported hypervisor) from the ISO and follow the guided setup. Veeam Backup & Replication is installed automatically.
- Complete the initial Veeam Software Appliance configuration wizard and set hostname, network settings, and admin credentials.

Connect Infrastructure to Veeam Backup & Replication

- Add your virtualization platform to Veeam Backup & Replication inventory (Backup Infrastructure > Managed Servers).
- Add at least one backup proxy. In smaller environments, Veeam Software Appliance can serve as the initial proxy.
- For VMware environments, configure Hot-Add transport mode. The proxy VM mounts the source disks via SCSI and reads them directly, thus avoiding the slower NBD path over the ESXi management network.

Deploy Veeam Infrastructure Appliance (Path A)

- Download Veeam Infrastructure Appliance OVA or ISO from the Veeam Customer Portal.
- Deploy using the same OVA/ISO process as Veeam Software Appliance. Select Hardened Repository or backup proxy as the target role during the configuration wizard.
- Once deployed, add Veeam Infrastructure Appliance to Veeam Backup & Replication as a managed server, then configure it as a backup repository or proxy.
- For the hardened repository role, add the repository in Veeam Backup & Replication (Backup Infrastructure > Backup Repositories) and set the immutability retention period.
- Skip this section if you're using Path B or Path C (since no Veeam Infrastructure Appliance is required).

What Veeam Software Appliance handles for you

Veeam Backup & Replication is pre-installed and ready to configure with no manual OS setup, software installation, or pre-deployment patching required.

Veeam Software Appliance ships pre-hardened, unnecessary services are disabled, the OS is locked down, and security best practices are applied by default.

Deploy as an OVA on VMware vSphere, boot the ISO on a physical server, or boot inside a VM on any other Veeam-supported hypervisor. No Linux experience is needed.

Install Veeam ONE

- Veeam ONE is a separate installer for Windows. It is not currently delivered as part of the appliance model.
- Install Veeam ONE on a Windows Server VM or physical host (see minimum requirements in the Veeam ONE deployment guide).
- Connect Veeam ONE to Veeam Backup & Replication and your vCenter/Hyper-V host during the setup wizard.
- Configure SMTP/email notification settings immediately after installation. You want alerts active from Day 1.

Milestone 3: First Backup Jobs

- Create your first backup job for your primary hypervisor. Target the Veeam Hardened Repository (Path A), the local repository on Veeam Software Appliance (Path B), or your existing NAS/Windows repository (Path C).
- Set a sensible retention policy to start: 14 daily restore points, 4 weekly, 3 monthly (GFS).
- Schedule the job to run during off-peak hours and verify it does not conflict with other maintenance windows.
- Run the job manually on first execution and monitor it through to completion.
- Confirm the job completes without warnings or errors before proceeding to Phase 2.

First restore test — do not skip!

Before moving to Phase 2, perform an Instant VM Recovery for a non-critical VM to confirm recoverability.

You are not protected until you have verified you can restore. This takes minutes and can prevent days of pain later.

What Veeam Infrastructure Appliance handles for you

Like Veeam Software Appliance, Veeam Infrastructure Appliance ships pre-hardened and pre-configured for its assigned role. No Linux administration is required after deployment.

A single Veeam Infrastructure Appliance serves one role: Veeam Hardened Repository or backup proxy. If you need both, deploy two appliances.

This has the same deployment formats as Veeam Software Appliance: OVA for VMware vSphere, or ISO for physical servers and other supported hypervisors.

PHASE 2 • Days 15–45

Optimize

Goal: Consistent protection, off-site copy, and visibility across the environment.

Milestone 4: Application-Aware Processing

Application-aware processing ensures crash-consistent backups become application-consistent too. This is critical for transactional workloads such as SQL Server, Oracle, Exchange, Active Directory, and other applicable workloads.

- Enable guest processing on backup jobs that cover Windows or Linux application servers.
- Configure application-aware processing for SQL Server, Oracle, Exchange, Active Directory domain controllers and other applicable workloads.
- Set a transaction log truncation policy where applicable and appropriate to your recovery needs.
- After the first application-aware job run, confirm restore points are marked application-consistent in Veeam Backup & Replication.
- Test a SQL database item-level restore (or other applicable workloads) using Veeam Explorer for SQL Server to confirm end-to-end application recovery works.

Milestone 5: Backup Copy and Vault

This milestone completes your 3-2-1 strategy: A local copy on your primary repository, plus an off-site immutable copy. This is the architectural cornerstone of your backup environment.

Connect Vault

- Add Vault as an object storage repository in Veeam Backup & Replication (Backup Infrastructure > Object Storage Repositories).
- Authenticate with your Veeam-issued credentials and select your region.
- Confirm immutability is enabled.

Backup copy jobs

- Configure backup copy jobs with a GFS retention policy to maintain longer-term restore points offsite.
- Verify off-site copy jobs complete successfully and confirm Vault objects show immutability flags in Veeam Backup & Replication.
- Perform a test restore from Vault to confirm the off-site copy is readable before declaring Phase 2 complete.

Path C: Offsite target options

Path A and B both target Vault for the off-site copy. Path C may use Vault or an alternative VCSP or third-party off-site repository if you have one already in place. Immutability is enforced by default on all Vault-stored backup data. If you target a non-Vault offsite, confirm immutability or object lock is configured on that repository.

Milestone 6: Monitoring, Alerting, and Orchestrator Setup

- Configure alarm notification recipients in Veeam ONE: Email alerts for job failures and missed service level agreements (SLAs).
- Define business hours in Veeam ONE to align SLA calculations with your operational schedule.
- Review default alarm thresholds: Disable or tune alarms irrelevant to your environment to avoid alert fatigue.
- Run your first Veeam ONE reports: Protected VMs report and job session report.
- Review the Unprotected VMs report and address any gaps identified before proceeding to Phase 3.

Install Veeam Recovery Orchestrator (Premium only)

Skip this section if your edition is Foundation or Advanced. Veeam Recovery Orchestrator is included only with Veeam Data Platform Premium.

- Veeam Recovery Orchestrator is a separate Windows-based installer. It can co-reside with Veeam ONE on the same Windows host or run on its own host.
- Install Veeam Recovery Orchestrator on a Windows Server VM or physical host. See minimum requirements in the Veeam Recovery Orchestrator deployment guide.
- During the setup wizard, connect Veeam Recovery Orchestrator to your Veeam Backup & Replication instance so it can take inventory of your existing backup chains.
- Connect Veeam Recovery Orchestrator to your vSphere, Hyper-V, or Microsoft Azure so your planned execution can power VMs and assign networks correctly.
- Optionally connect Veeam Recovery Orchestrator to Veeam ONE for richer monitoring data and DataLab-based verification.
- Apply your Veeam Data Platform Premium license to activate Veeam Recovery Orchestrator.
- Configure SMTP/email so planned execution notifications work from Day 1.

PHASE 3 • Days 46–75

Data and Business Resilience

Goal: Close protection gaps, improve RTOs/RPOs, and add ransomware resilience.

Milestone 7: Close Coverage Gaps

- Run the unprotected VMs report in Veeam ONE to address all unprotected workloads before any other tuning.
- Extend protection to physical workloads using Veeam Agent for Microsoft Windows or Veeam Agent for Linux as needed.
- Review job schedules for conflicts and stagger start times to prevent proxy and repository resource contention.
- Validate RPO compliance: Are all critical VMs generating restore points within your target recovery window?
- Confirm all jobs are completing within your defined backup window.

Adding proxy capacity with a second VIA

If backup jobs are running slowly or overrunning their backup window, deploy a second Veeam Infrastructure Appliance in the proxy role.

The pre-hardened appliance model makes this fast: Deploy the OVA or ISO, register it in Veeam Backup & Replication, and jobs will automatically load-balance across both proxies with no manual proxy configuration required.

Milestone 8: Ransomware Readiness

- Veeam Data Platform Advanced and Premium ship with two complementary security tools. The first is Recon, which is Veeam's threat-intelligence service that surfaces IOCs and emerging data drawn from real-world incident response. The second is scan backup, an in-product action in Veeam Backup & Replication. It examines existing backup chains for malware indicators and validates file integrity, without requiring an isolated network or booting VMs.

Run a scan backup:

- Create a SureBackup job in Veeam Backup & Replication under Home > SureBackup. SureBackup runs as a scheduled job and can scan your backups for malware, signature-based threats, and file integrity in one flow without requiring an isolated network or VM boot required for the scan itself.
- Link the backup jobs you want covered so that over time the SureBackup job spans all your data: Veeam Hardened Repository (Path A), Veeam Software Appliance local repository (Path B), the existing NAS/Windows repo (Path C), and Vault.

- In the verification options, enable malware scan with Veeam Threat Hunter (or a third-party antivirus solution) to check backup content against a current threat-signature database.
- In the same verification options, enable file integrity check to validate the backup file with a CRC check to identify corrupt blocks.
- Schedule the SureBackup job and review the session results regularly; investigate any flagged restore points before using them for recovery.
- For an ad hoc check between scheduled runs, go to Home > Backups, expand the backup job, select the workload, and choose Scan Backup from the Backup tab.

Install Recon

- Install the Recon binary on any Windows-based Veeam infrastructure host or any Linux host of your choice.
- Recon can also be installed on applicable Windows domain controllers.
- Recon cannot be installed on Veeam Infrastructure Appliance. Veeam Infrastructure Appliances are single-role and pre-hardened.

Immutability audit

- Confirm the immutability period on your Veeam Infrastructure Appliance hardened repository is set to an appropriate retention window.
- Review backup encryption settings and enable at-rest encryption on jobs if not already configured.
- Run the Veeam ONE "Immutable Workloads" report to measure and identify workload backup immutability targets.

Ransomware recovery readiness

Document a simple recovery runbook that includes which VMs to restore first, from which restore points, and to which target.

Identify at least one clean, pre-infection restore point in Vault as your last known good anchor.

Your immutable copies cannot be overwritten or encrypted during the immutability period. This is your safety net.

Path A: Veeam Hardened Repository plus Vault.

Path B: Veeam Software Appliance local storage plus Veeam Vault.

Path C: Vault plus your local repository if you have configured immutability there.

Milestone 9: Performance Tuning and Orchestration Plans

- Review proxy throughput in Veeam Backup & Replication job statistics. If jobs are bottlenecked, deploy a second Veeam Infrastructure Appliance in the proxy role.
- Confirm backup transport mode is optimal: Hot-Add (VMware) or Direct Storage Access where available.
- Validate that all backup jobs are complete within your defined maintenance window.
- Review Veeam ONE performance charts and identify VMs with unusually high change rates that may benefit from dedicated jobs or adjusted schedules.

Build Initial Orchestration Plans (Premium Only)

Skip this section if your edition is Foundation or Advanced, or if you are not using a supported hypervisor for Veeam Recovery Orchestrator.

Veeam Recovery Orchestrator turns your manual recovery runbook into an executable plan. Building plans now means Phase 4 can prove recoverability automatically rather than rerunning manual restores.

- Identify Tier 1 application stacks that need orchestrated recovery (e.g., domain controllers, primary database, primary application servers).
- In Veeam Recovery Orchestrator, create your first restore plan covering one of those stacks.
- Define your VM start order and dependencies so prerequisites (e.g., DCs, DNS, etc.) come up before dependent services.
- Configure recovery targets (e.g., host, cluster, datastore) and network map the production network for actual failover, and an isolated network for testing.
- Set the plan's RTO and RPO objectives so Veeam Recovery Orchestrator can flag drift over time.
- Save the plan and review the auto-generated documentation with stakeholders before declaring Phase 3 complete.

PHASE 4 • Days 76–100

Prove Value and Operationalize

Goal: Verify recoverability, establish ongoing hygiene, and demonstrate ROI.

Milestone 10: Recovery Testing

The only backup that matters is one you can restore from. Phase 4 is where you prove — with documented evidence — that your environment meets its RTO and RPO commitments.

SureBackup and scan backup

- Configure a SureBackup Application Group that covers your most critical VMs (e.g., domain controllers, key application servers).
- Run a SureBackup job to automate boot verification and confirm VMs start and pass heartbeat, ping, and application-level tests.
- For a lighter-weight verification pass, run a Scan Backup. It validates file integrity and checks for threats without booting VMs, which is a practical complement or alternative to SureBackup in smaller environments.

Granular and full restore tests

- Test file-level restores and recover individual files from a backup to a test location.
- Test application item recovery by restoring a SQL database object or Active Directory user using Veeam Explorers.
- Test a full VM restore from Vault to simulate total on-premises loss to validate your off-site copy.
- Record actual recovery times and compare them against your RTO targets and document the results.

Recovery testing best practice

Always restore to a non-production target and never overwrite live workloads during a test.

Document what was restored and from which restore point, to which target, and how long it took.

These results are your proof of recoverability. Retain them for compliance reviews, audits, and management reporting.

Run orchestration plans (Premium only)

Skip this section if your edition is Foundation or Advanced, or if your hypervisor is not supported by Veeam Recovery Orchestrator. Phase 3 built your first restore plan, but Phase 4 is where it earns its keep.

- Run an unattended readiness test on your plan. Veeam Recovery Orchestrator checks restore-point availability, target capacity, and configuration drift, without having to boot any VMs.
- Run a DataLab test on your plan. Veeam Recovery Orchestrator restores the application stack into an isolated network and runs application-level verification checks against live VMs.
- Record actual recovery times from the DataLab run and compare them to the RTO target you set in Phase 3.
- Generate the Veeam Recovery Orchestrator recovery readiness report and archive it alongside your other recovery test results.
- For workloads not covered by a Veeam Recovery Orchestrator plan, fall back to the manual restore tests above.

Milestone 11: Reporting and Documentation

Generate a monthly Veeam ONE Executive Summary report and share with management to demonstrate backup health and coverage.

- Export a protected workload inventory report to confirm coverage scope.
- Document your final backup architecture, including job list, repository layout, Veeam Infrastructure Appliance roles, schedules, and retention policies.
- Review Veeam Vault storage consumption and confirm your usage aligns with your expected budget.
- Archive recovery test results alongside architecture documentation.
- Premium only: Generate the Veeam Recovery Orchestrator recovery readiness report each month. Track the readiness score over time as workloads and dependencies change.
- Premium only: Archive Veeam Recovery Orchestrator-generated plan documentation alongside your architecture docs. Veeam Recovery Orchestrator regenerates this automatically when plans change, so re-archive when plans are updated.

Milestone 12: Ongoing Hygiene Cadence

By Day 100, your environment should be stable and fully documented. These habits keep it that way:

- **Weekly:** Review your Veeam ONE job health dashboard and address failures or warnings quickly.
- **Weekly:** Review the unprotected VMs report in Veeam ONE and add coverage for anything new.
- **Monthly:** Run an executive summary and protected VMs reports and share results.
- **Monthly:** Review Vault storage consumption and growth rate. Flag if you're trending past your budgeted footprint or upcoming retention bumps.
- **Monthly:** Confirm retention windows are still active and unmodified.
- **Quarterly:** Perform a documented recovery test and rotate workload types.
- **Quarterly:** Run a scan backup pass across each repository to check for malware signatures and file-integrity drift.
- **Quarterly:** Review who has administrative access to Veeam Backup & Replication, Veeam ONE, and Veeam Recovery Orchestrator (Premium only). Remove access for anyone who has changed roles or left.
- **Quarterly (Premium only):** Run a Veeam Recovery Orchestrator DataLab test and rotate which orchestration plan is exercised.
- **Quarterly (Premium only):** Regenerate and archive Veeam Recovery Orchestrator plan documentation if any plans have changed since last review.
- **Monthly:** Review Recon threat intelligence updates and apply relevant signatures or rules to your environment.

- **Annually:** Review your backup architecture and retention policies against current business requirements and any new compliance obligations.
- **Annually:** Perform a full restore from Vault to validate the off-site copy is recoverable end-to-end. Document the result.
- **Annually:** Review encryption settings in-flight and at-rest and rotate keys per your security policy.
- **As needed:** Plan your Veeam component update cadence (e.g., Veeam Software Appliance, Veeam Infrastructure Appliance, Veeam ONE, Veeam Agents, and Veeam Recovery Orchestrator if applicable) and subscribe to release notifications.
- **Before renewal:** Review licensing usage, growth projections, and edition fit. If you've grown past your edition's feature set, this is the moment to discuss an upgrade with your Veeam representative.

Closing Recommendations

Congrats! You Did It.

In 100 days, you went from deployment to a fully operationalized data protection environment. Your workloads are protected, your backups are hardened and immutable, and you've proven you can recover not just in theory, but on record.

That's not a small thing.

Now the focus shifts from building to maintaining. Keep restores on a regular testing schedule, tune policies as your environment evolves, and use your monitoring and reporting cadence to catch drift before it becomes risk. The habits you established in Milestone 12 — your weekly, monthly, quarterly, and annual hygiene cadence — are what keep your environment honest long after Day 100. Follow them, own them, and evolve them as your organization grows.

Remember, Day 100 isn't the finish line. It's the baseline. Resilience is a practice, not a project.

Keep your admin roles current so the right people always have the right access, and stay subscribed to Veeam release notes and security advisories so you're never caught off guard.

You Don't Have to Do This Alone

Veeam's communities, learning resources, and technical teams exist to help you go further. Tap into them as your environment grows and matures! A curated list of resources is available in the appendix.

For questions or next steps, reach out to your Customer Success Account Manager, or contact Veeam Technical Support for technical queries.

Appendix: Quick Reference

Key Components: Veeam Data Platform

- **Veeam Software Appliance:** A pre-hardened appliance with Veeam Backup & Replication pre-installed. Deploy as OVA (VM) or ISO (physical). This is the recommended starting point for all SMB deployments.
- **Veeam Infrastructure Appliance:** A pre-hardened appliance deployed as a dedicated backup proxy or hardened repository. It provides local immutability without Linux expertise with one role per appliance.
- **Veeam Backup & Replication:** A core backup engine, hosted on Veeam Software Appliance. It manages jobs, repositories, proxies, and recovery operations.
- **Veeam ONE:** This does monitoring, alerting, and reporting. It has a separate Windows-based install and connects to Veeam Backup & Replication and your hypervisor for full-stack visibility.
- **Recon:** This is Veeam's threat-intelligence service. It surfaces indicators of compromise (IOCs), threat signatures, and emerging-campaign data drawn from real-world incident response. Included with Veeam Data Platform Advanced.
- **Scan backup contents:** This is an in-product action that scans existing backup chains for known malware signatures and validates file integrity without requiring an isolated network or booting VMs. Included with Veeam Data Platform Advanced.
- **Veeam Recovery Orchestrator:** An orchestration platform that automates application-level disaster recovery (DR). It lets you build executable restore plans, run readiness tests, perform DataLab-based verification and generate recovery documentation. Included with Veeam Data Platform Premium.
- **Veeam Data Cloud Vault:** This provides immutable cloud object storage for off-site copies. It's Veeam-managed with no separate cloud account required.

Key Terms

- **Recovery point objective (RPO):** Maximum acceptable data loss, measured in time. Drives backup schedule frequency.
- **Recovery time objective (RTO):** Maximum acceptable downtime before a workload must be recovered.
- **Grandfather-Father-Son (GFS):** Retention scheme maintaining daily, weekly, and monthly restore points.
- **Immutability:** Backup data that cannot be modified or deleted for a defined retention period. Protects against ransomware encryption of backup files.
- **Instant VM Recovery:** Restores a VM directly from a backup in seconds without copying data first. Always migrate to production storage after validation.
- **Orchestration plan (Veeam Recovery Orchestrator):** An executable runbook that defines the order, dependencies, target locations, and network mappings for restoring a set of workloads. Replaces a manual recovery runbook with auto-documented and testable automation.
- **DataLabs:** An isolated test environment in which Veeam Recovery Orchestrator (or SureBackup) restores a backup and runs application-level verification without affecting production. Enables full plan testing at any cadence.
- **Application-aware processing:** Guest processing that creates application-consistent backup points for SQL Server, Oracle, Exchange, Active Directory, SharePoint, PostgreSQL, and MySQL. Uses VSS on Windows and pre-freeze/post-thaw scripting plus database-native quiescing on Linux.
- **Veeam Hardened Repository:** A Linux-based backup repository with immutability enforced at the filesystem level. Veeam Infrastructure Appliance delivers a Veeam Hardened Repository pre-configured with no Linux administration required. Object storage and object lock are separate immutability mechanisms, not Veeam Hardened Repositories. File system-level immutability protects against in-OS attacks but not VM-level destruction. A Veeam Hardened Repository running as a virtual appliance can still be deleted at the hypervisor layer, so deploy Veeam Infrastructure Appliance on physical hardware for maximum protection.
- **Hot-add transport mode:** This is VMware-specific backup transport. The proxy VM hot-adds the source VM's virtual disks and reads them via SCSI, avoiding the NBD path over the ESXi management network.

Appendix: Useful Links

My Account

Your Veeam Account is your central hub for managing your deployment. Once logged in, you can download products and license keys, manage case administrators, contact Veeam support, and renew contracts or add licenses.

- Log in or create your Veeam Account
- How to create an account
- Sign-in FAQ
- License and/or case admin roles management

Documentation and Downloads

- Help Center with technical documentation, deployment guidance, and user guides
- Product Downloads, including software updates, patches, and release notes
- Support Knowledge Base with common issues, troubleshooting steps, and recommended resolutions, regularly updated by Veeam Support and Engineering teams

Learning and Best Practices

- Live Onboarding Webinars: Regular live onboarding webinars where you can ask questions in real time and hear directly from technical specialists
- Veeam University Free: Self-paced courses and certifications at no cost
- Veeam Sizing Calculators: online sizing and estimation tool used to calculate infrastructure, storage, and capacity requirements for Veeam deployments
- Best Practices by Veeam Solution Architects: Infrastructure design and configuration guidance drawn from real-world deployments, which is worth revisiting as your environment matures
- Actionable Prompts for Veeam Intelligence: A curated collection of effective prompts to help you unlock the full potential of Veeam Intelligence
- Veeam Search: Veeam's centralized search portal for searching across Veeam resources from one place

Veeam Communities

- Veeam Community Forums: connect with peers, share best practices, attend User Groups and community events, and discuss real-world use cases
- Veeam R&D Forums: your direct line to Veeam R&D for product discussions, technical questions, and feature feedback

About Veeam Software

Veeam is the Data and AI Trust Company, specializing in helping organizations ensure their data and AI are fully understood, secured, and resilient to enable the acceleration of safe AI at scale. As the market leader in both data resilience and data security posture management, Veeam is built for the convergence of identity, data, security, and AI risk.

Headquartered in Seattle, with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 82% of the Fortune 500.

Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.