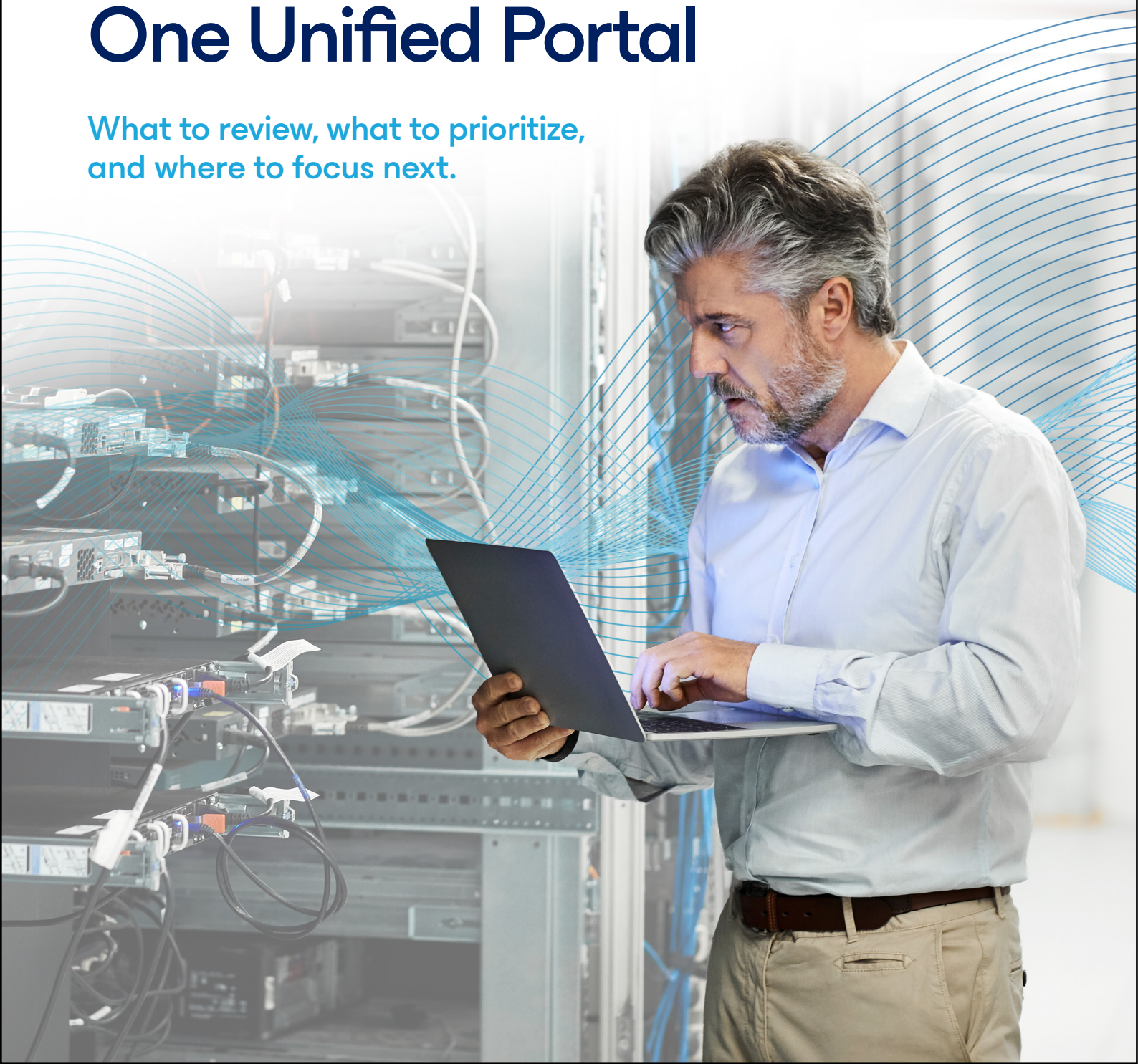
VEEAM DATA CLOUD

Optimization Guide: Get More from your Cloud Environment in One Unified Portal

What to review, what to prioritize, and where to focus next.



Program Overview

This guide is for teams who have completed onboarding and are ready to maximize the value of Veeam Data Cloud. If you run into an issue along the way, open a case with Veeam Support.

Optimizing goes beyond checking that your backups are complete. It also means making sure that:

Protection keeps pace with change, so new users, apps, and cloud resources are never left out.

Recovery is fast and proven, because your team has practiced real incident scenarios.

You use every feature you are entitled to, from threat detection to service level agreement (SLA) monitoring.

This guide provides a detailed description for each part of the program and gives examples of goals and targets. Please see the last page of this document for details on how opportunities transacted through the enterprise license program are paid rebates outside of the standard program.

How to use this guide:

- Start with the six optimization habits. They apply to every workload.
- Jump to the workloads you protect right now by using the menu on the next page. Each section shows the top three actions to take in order.
- Look at the workloads you don't protect yet to see what the full potential of Veeam Data Cloud can add.
- Use the optimization rhythm to keep everything current.

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

Your Veeam Data Cloud platform

Veeam Data Cloud brings **Microsoft 365, Microsoft Entra ID, Microsoft Azure, and Salesforce** protection into one unified portal. This gives you one dashboard and one view of your protected and unprotected objects, and one place to monitor backup and restore sessions across your environment.

Select a workload to go straight to its section:

Workload	Top optimization focus	Go to section
Optimization habits (all workloads)	• Coverage, health, entitled features, and recovery drills	Start here
Microsoft 365	• Learn about Advanced Threat Detection • Tune policy scope and retention to fit how you work currently	Microsoft 365
Microsoft Entra ID	• Prioritize your critical identity objects • Use property-level restore for configuration changes • Put logs, exports, and BitLocker keys to work	Microsoft Entra ID
Microsoft Azure	• Close coverage gaps on the resources page • Test recovery to a new location • Check backup requirements before changing your architecture	Microsoft Azure
Salesforce	• Fine-tune backup frequency and retention by object • Compare before you restore • Put notifications to work and prepare for metadata recovery	Salesforce
Optimization rhythm	• Weekly, monthly and quarterly reviews	Go

Protecting only some of these workloads?

Each workload you add appears in the same unified portal, with the same dashboard, policy view, and reporting. There's no new tool to learn, and one place to prove your protection to auditors and leadership. Read the sections for workloads you haven't yet protected to see what you could add, then talk to your Veeam account team. You can also explore the full Veeam Data Cloud platform or take the product tour.

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

Start here: Six optimization habits

These habits move you from “backups are running” to “protection is optimized”, and can apply to whichever workloads you protect.

1 Check your coverage against today’s environment

Your environment has changed since you onboarded. Use the organization dashboard to compare your protected and unprotected objects with what exists today and bring anything new that matters into scope. An object counts as protected only when a restore point exists within the recovery point objective (RPO) set by its policy. Organization dashboard

2 Turn warnings into action

Don’t let warnings become normal. Review sessions that completed with warnings or errors each week and fix the root cause of these warnings, since they can affect recoverability and your RPO.

3 Activate the features you’re entitled to

Each workload section lists features you may not be using yet, such as Microsoft 365 threat detection, Entra ID property-level restore, or Salesforce comparison.

4 Give people only the access they need

The first person invited to Veeam Data Cloud becomes the OrganizationAdmin, with full control of every workload and tenant. Over time, many users may end up with full admin rights when they really only need enough access to restore data or check backups. Review who currently has access to your account and give each person a role that matches their job.

- Keep OrganizationAdmin credentials to a small group of named owners. Under Settings > Users, check who has OrganizationAdmin access.
- Give everyone else viewer access plus a workload role. Each workload offers roles such as administrator, backup operator, restore operator, and viewer. For example, your service desk can restore data without full admin rights.
- Limit each role to the tenants that a specific person manages. When you add a new tenant, update those role limits so that the right people can reach it.
- Assign roles through groups if you use Microsoft Entra ID single sign-on (SSO), so new team members get the right access automatically.
- Remove access for people who have left or changed jobs.

Learn more: Roles

Back to the workload menu

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

5 Move from one-off restores to recovery drills

You ran a first restore during onboarding. Now, practice the incidents you're most likely to face, such as ransomware, an unwanted policy change, or a lost region, and time how long it takes to find and restore that data.

6 Learn from your restore history

Review recent restore sessions. What took the longest to find? What needed a second attempt? Use the answers to choose your next drill and update your runbooks.

Microsoft 365

Veeam Data Cloud *for Microsoft 365* protects Exchange Online, SharePoint Online, OneDrive, and Teams.

> **Your optimization goal**
>
> Move from *"our Microsoft 365 tenant is backed up"*
> to **"our Microsoft 365 data is protected to meet our business needs, is easy to find, ready to restore, and monitored for threats."**

STEP 1

Use Advanced Threat Detection for ransomware detection

Why it matters: This step helps you recover with greater confidence by identifying signs of malware and ransomware in your Microsoft 365 backups and allows you to select a clean restore point. Veeam's ransomware detection uses individualized behavioral profiles and anomaly detection to identify potential ransomware activity at the earliest possible stage. The threats page brings ransomware detections and Microsoft-provided malware alerts all together in one place.

What to do:

- **Foundation edition:** Advanced Threat Detection is available with the Advanced or Premium plans. Talk to your account team about upgrading.
- **Advanced or Premium edition:** Advanced Threat Detection is included, but it only runs after an administrator agrees to the AI terms in the AI consent settings (settings icon > AI). Changes can take up to 24 hours. After changes complete, open the threats page and use the malware threats and ransomware threats tabs to review any flagged threats, identify anything that needs to be resolved, and make sure someone on your team owns the review and the handoff to security.

Keep in mind

Ransomware detection needs about 45 days of backup history per workload to build a reliable baseline. Learn more: Microsoft 365 threats

Back to the workload menu

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

STEP 2

Tune your policy scope and retention to how you work today

Why it matters: Your organization has changed since onboarding. New users, sites, and teams appear every week, and different teams need data to be kept for different lengths of time.

What to do:

- Replace static user lists with dynamic, group-based backup rules so new users are protected automatically. Users added this way consume licenses, and usage above your contracted quantity is billed as overage, so check with your account team before you widen scope.
- Revisit retention with legal and compliance. The default cadence is once per year. This can be increased, but to avoid data deletion, it cannot be decreased. Therefore, make sure all teams agree to the changes before you make them.
- Enable **All Versions** for SharePoint sites, Teams, and OneDrive locations that need to be protected. By default, only the latest version is backed up.
- Using express backup on the Premium plan? Its retention is fixed, so the retention and item-version settings above apply to your standard (Flex) policies only.

Learn more: Licensing | Data backup

STEP 3

Set up scheduled reports and notifications

Why it matters: Protection drifts quietly. Scheduled reports and alerts show your team any failed backups, unprotected users, license changes, and restore activity without anyone having to log in and check.

What to do:

- Go to **Reports > Add a Scheduled Report.** Start with a weekly **Backup Summary Report** and **User Protection Report** to spot failed policies and unprotected users, plus a monthly **Restore Activity Report** for audit.
- In **Settings > Notifications,** add email recipients for **Backup Failed, License Changes,** and **Restore Activity.** You can also send backup and restore alerts to a Teams channel through an incoming webhook.
- Add **no-reply@mail.cloud.veeam.com** to your safe senders list. Report links are valid for 7 days, and recipients need a Veeam Data Cloud login to download them.

Learn more: Scheduling reports | Managing notifications

Back to the workload menu

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

Features you may not be using yet:

- Advanced Threat Detection (Advanced and Premium plans)
- Dynamic Entra ID groups for backup scope
- All-version backup for SharePoint, OneDrive, and Teams
- Advanced search with restore or download
- Scheduled protection and backup reports
- Role-based access control (RBAC) for delegated restores
- Backup, license, and restore notifications (email and Teams)

You're optimized when:

- ✓ Advanced Threat Detection is on (if eligible) and has a named owner.
- ✓ Dynamic Entra ID groups protect new users automatically.
- ✓ Retention and item version needs are agreed upon and configured.
- ✓ Scheduled reports and failure and license alerts go to a named owner.

Not protecting Microsoft 365 yet?

Protect Exchange Online, SharePoint Online, OneDrive, and Teams in the same console you already use, with threat detection, advanced search, and flexible retention.

Explore Microsoft 365 protection • Take the product tour • Talk to your account team

Back to the workload menu

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

Microsoft Entra ID

Veeam Data Cloud *for Microsoft Entra ID* protects Entra ID tenant data, audit logs, and interactive sign-in logs, including users, groups, administrative units, roles, applications, service principals, conditional access policies, in-tune policies, in-tune role-based access control (RBAC) roles, organizational contacts, and devices, including BitLocker recovery keys.

> **Your optimization goal**
>
> Move from *"our identity tenant is backed up"*
> to **"we can recover critical identity objects quickly, investigate what changed, and respond to unwanted changes or deletions."**

STEP 1

Prioritize your critical identity objects

Why it matters: Veeam Data Cloud backs up every object type in your policy scope, but an identity incident can lock people out of every business application. Knowing which objects matter most, and who owns them, tells you what to recover first.

What to do:

- List privileged and break-glass accounts, key groups, roles, administrative units, enterprise applications, and service principals.
- Check that your backup policy includes the optional object types, such as conditional access policies, in-tune policies, in-tune RBAC roles, organizational contacts, and devices, and add any that are missing.
- For each, record a business owner, a technical owner, and how you will check it works after a restore.

Learn more: Entra ID protection

STEP 2

Use property-level restore for configuration changes

Why it matters: Most identity issues are unwanted changes, not deletions. Restoring only the affected properties fixes the problem while keeping the current settings that are still correct.

What to do:

- When a setting changes unexpectedly, restore the affected properties instead of the whole object.
- Practice on a non-production conditional access or in-tune policy.
- Add property-level restore to your identity incident runbook, alongside full-object restore for deletions.

Learn more: Entra ID restore

Back to the workload menu

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

STEP 3

Put logs, exports, and BitLocker keys to work

Why it matters: Recovering an object is only half of an identity incident. Your security team also needs to know what changed and when.

What to do:

- Export audit and sign-in logs to support security investigations. Exports are delivered as a download link that is valid for two hours and opens in Azure Storage Explorer.
- Export objects to JSON to review a previous configuration before restoring critical policies or applications.
- Give authorized service desk staff a documented way to view and copy BitLocker recovery keys. BitLocker key backup requires the BitlockerKey.Read.All permission, so confirm it was granted when your tenant was added.

Learn more: Entra ID log export



Features you may not be using yet:

- Property-level restore
- Optional object types: Conditional access, in-tune, organizational contacts, and devices
- Audit and sign-in log export
- JSON export of tenant objects
- BitLocker recovery-key access



You're optimized when:

- ✓ Critical users, groups, roles, apps, and policies are listed with owners
- ✓ Optional object types (conditional access policies, in-tune policies, in-tune RBAC roles, organizational contacts, and devices) are included in your backup policy
- ✓ Property level restore has been practiced on a policy
- ✓ Log and JSON export have a defined security use and owner
- ✓ BitLocker key retrieval is in service desk procedures



Not protecting Microsoft Entra ID yet?

Identity controls access to Microsoft 365, Azure, and your SaaS apps. Protect it in the same console you already use and recover both access and data from one place. Already on the Microsoft 365 Advanced or Premium plan? Entra ID protection may already be included.

Explore Entra ID protection · Take the product tour · Talk to your account team

Back to the workload menu

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

Microsoft Azure

Veeam Data Cloud *for Microsoft Azure* protects Azure VMs (image-level), virtual disks, Azure SQL databases, Cosmos DB accounts, and Azure Files snapshots.

> **Your optimization goal**
>
> Move from *"our Azure resources have policies"*
> to **"we can see coverage across Azure, match protection to each resource type, and recover every critical application at the level it needs."**

STEP 1

Close coverage gaps on the resources page

Why it matters: New resources get created outside the original policy scope. A monthly check catches them before an incident does.

What to do:

- On the resources page, filter by unprotected to identify discovered VMs, Azure SQL databases, Cosmos DB accounts, and Azure file shares that do not have a backup policy.
- Export the list to CSV and compare it with your cloud operations inventory.
- Review new regions and resource groups after each application deployment.

Learn more: Viewing Azure resources

STEP 2

Test recovery to a new location

Why it matters: If the original resource or region is unavailable, restoring to the original location is not an option. Test the alternative before you need it.

What to do:

- Pick one Tier 1 application and restore it to a new location in a controlled test.
- Check networking, access, dependencies, and that the application works.
- Update your runbook with what you learned, then clean up test resources.

Back to the workload menu

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

Resource	Recovery options
Azure VM	Restore VM to original or new location
Virtual disk	Restore disk to original or new location
Azure SQL	Restore database to original or new location
Cosmos DB	Restore entire account or selected items
Azure Files	Restore files from an Azure file share to the original or new location

Learn more: **Azure protection**

STEP 3

Check backup requirements before changing your architecture

Why it matters: Some Azure settings can block backup or restore operations. Bring backup into your cloud governance reviews so changes don't create silent gaps.

What to do:

- Restores can fail when Azure policies block tag assignment, and locked VMs and disks cannot be restored.
- Cosmos DB accounts with periodic backup or multi-region writes are not supported for backup.
- Azure Files backup is not supported when the storage account uses network restrictions. Tip: Enable Azure Files soft delete to protect snapshots from accidental deletion.

Learn more: **Azure considerations and limitations**

Back to the workload menu

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

Features you may not be using yet:

- Unprotected resource filter and CSV export
- New location restore
- Cosmos DB restore of entire accounts or selected items

You're optimized when:

- ✓ Unprotected resources are reviewed monthly
- ✓ Every critical application has an owner and a documented restore scope
- ✓ A new location restore has been tested for a Tier 1 application
- ✓ Backup requirements are part of architecture and governance reviews

Not protecting Microsoft Azure yet?

Protect Azure VMs, SQL databases, Cosmos DB. and Azure Files in the same console you already use, with coverage reporting and new location restore.

Explore Azure protection · Take the product tour · Talk to your account team

Note: This section applies to Veeam Data Cloud for Microsoft Azure on the unified experience platform. If you use the original platform, follow its own documentation.

Back to the workload menu

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

Salesforce

Veeam Data Cloud for Salesforce protects Salesforce files, data, and metadata.

> **Your optimization goal**
>
> Move from *"our Salesforce organization is backed up"*
> to **"we protect high-value objects at the right frequency, keep them as long as needed, check changes before restoring, and can recover both data and metadata."**

STEP 1

Fine-tune backup frequency and retention by object

Why it matters: Not every object needs the same protection. Opportunities, cases, or custom objects that change often may need more frequent backups than static data.

What to do:

- Group objects: Business-critical and high change, standard operational, long-term retention, and configuration/metadata.
- Use high-frequency backups only for objects with a tight recovery point need and set different schedules for the rest.
- Set object-level retention, and archive data that is no longer needed day to day but must be kept for compliance.

Learn more: Salesforce protection

STEP 2

Configure Archival policies with Enroll Package

Why it matters: This step helps large Salesforce environments reduce their Salesforce storage. You choose which data to archive, and the data is then stored in Veeam and can be restored back to the Salesforce tenant when needed.

What to do:

- Install "Enroll Package" in the Salesforce tenant.
- Choose what data to archive and how often.
- Data is still stored in Veeam at no additional cost.
- Users can view and restore archived records directly in Salesforce, without signing into Veeam Data Clou

Learn more: Salesforce Archiving

Back to the workload menu

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

STEP 3

Put notifications to work and prepare for metadata recovery

Why it matters: Many Salesforce issues come from configuration changes, not deleted records. Restoring data alone won't fix a broken flow or profile.

What to do:

- Route real-time notifications for backup, recovery, connection issues, archival, encryption, and protected data changes to a named owner.
- Practice restoring object hierarchies and parent/child relationships, not just single records.
- Practice restoring metadata such as reports, profiles, permission sets, and flows.

Learn more: Salesforce protection

Features you may not be using yet:

- Per-object schedules and high frequency backup
- Object-level retention and archiving
- Data archival
- Real-time notifications

You're optimized when:

- ✓ Objects are grouped by importance, with schedules and retention to match
- ✓ Archival policies are configured
- ✓ Hierarchy and metadata recovery have both been practiced
- ✓ Notifications are configured for all relevant stakeholders and changes

Not protecting Salesforce yet?

Protect Salesforce data and metadata in the same console you already use, with per-object schedules, comparison before restore, and real-time notifications.

Explore Salesforce protection · Take the product tour · Talk to your account team

Back to the workload menu

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

Your optimization rhythm

Optimization isn't a one-time project. Use this schedule to keep your protection aligned with your environment, across every workload, from one console.

When	What to review	Result
Weekly	Failed and warning sessions Microsoft 365 active threats (if enabled)	Issues are fixed before they affect recovery
Monthly	Protected vs. unprotected objects and resources Recent restore points Usage and capacity trends	Coverage keeps pace with your environment
Quarterly	Policy scope, retention and recovery owners At least one recovery drill per workload	Recovery plans stay current and proven
After a major change	New apps, regions, accounts, subscriptions, departments, or SaaS configuration	New critical assets are protected from day one
After an incident	Time to find data, time to restore, and what to improve	Every incident makes the next recovery faster

Need a hand?

All support options

Veeam Data Cloud: Getting Support

Product guidance

Veeam Data Cloud technical documentation

Expert guidance and expanding your environment

Connect with a Technical Account Manager (TAM) to review your environment and set optimization priorities.

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 DSPM, Veeam is built for the convergence of identity, data, security, and AI risk. Headquartered in Seattle, with offices in 30+ countries, Veeam protects over 550,000 customers worldwide, including 80% of the Fortune 500. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.

Keep this guide handy

Your environment will keep changing, and so will Veeam Data Cloud. Come back to this guide whenever you add users, applications, cloud accounts, or new workloads.

Back to the workload menu

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