# Veeam Data Cloud *for Microsoft 365*

## Technical White Paper

A Deep Dive into Architecture, Security, and Compliance

# Contents

# Introduction

## Summary

This document is designed to assist backup administrators and IT professionals with understanding the technical aspects of Veeam Data Cloud *for Microsoft 365*. It also provides insights into the architectural components, security protocols, and compliance certifications that make up the solution.

With Veeam Data Cloud *for Microsoft 365*, you get a cloud-hosted backup service which is purpose-built to protect Microsoft 365 data. This includes Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams. It is also part of Veeam Data Cloud Platform, which supports Salesforce, Entra ID, Azure, and Veeam Vault as well.

If you have any questions or would like to see a custom demo of this solution at any point, you can contact us at this web page.

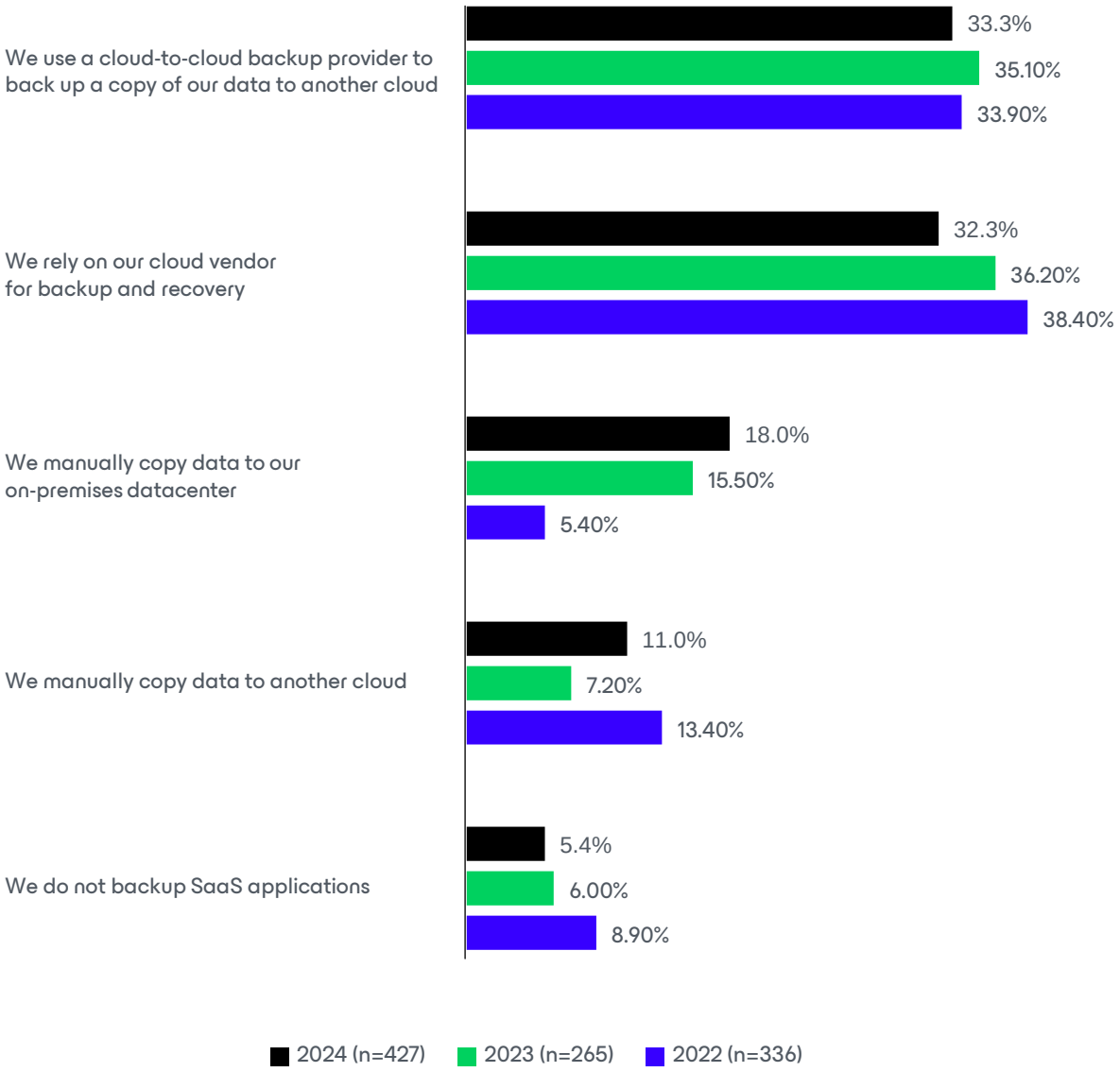
## The Market View of Microsoft 365 Data Protection

Microsoft 365 backup has come a long way in the last four to five years. As the criticality of Microsoft 365 data has grown, so has the perceived need to ensure its protected. In fact, Microsoft's own entrance into the Microsoft 365 backup market has added to the growing perception that this data should be protected. However, in a recent survey conducted by 451 Group, it was found that ~65% of organizations are not properly protected. As of 2024, 33% chose to back up via a backup provider, while the remaining did not feel that backing of SaaS applications was their responsibility or utilized very manual internal processes to retain their data. This research indicates that there is still a lack of understanding that many organizations have when it comes to their responsibility for protecting Microsoft 365 data. According to Gartner, 75% of enterprises will prioritize backup of SaaS applications like Microsoft 365 as a critical requirement by 2028, compared with only 15% in 2024. This forecasts massive adoption in the next few years as organizations search for ways to protect this critical data.

Sources: 451 Group, Voice of the Enterprise: Storage, Disaster Recovery 2024.

Gartner Top Trends for Enterprise B&R for 2024, Veeam Cloud Protection Trends Report 2024

**What is Your Organization's Primary Data Protection Strategy for SaaS Applications (e.g., Salesforce, Microsoft 365, Google Workspace [formerly G Suite], etc.)?**



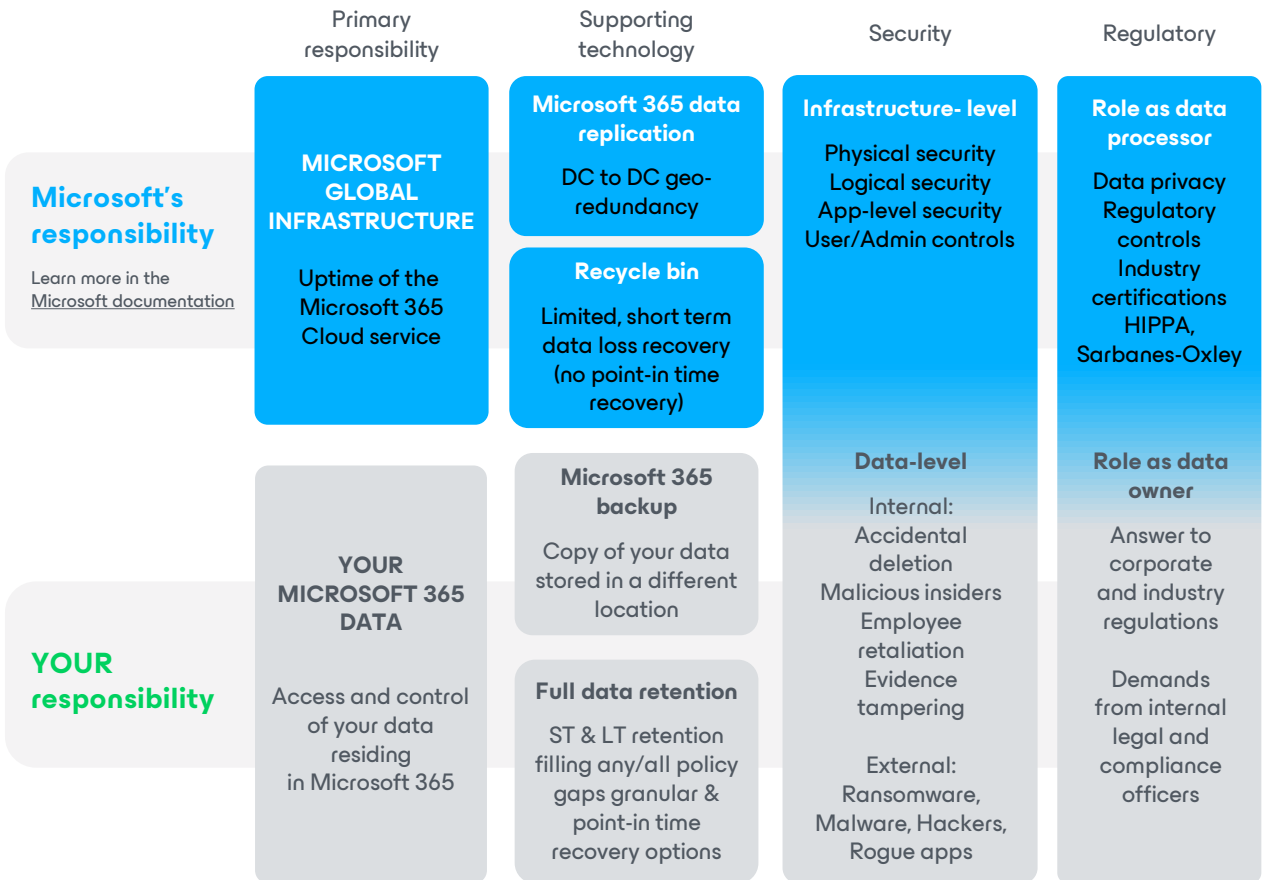

Source: 451 Group, Voice of the Enterprise: Storage, Disaster Recovery 2024

## The Shared Responsibility Model

Organizations prioritize the protection of Microsoft 365 data for various compelling reasons, but the key to understanding this critical requirement is rooted in the Shared Responsibility Model. This model is utilized by cloud service providers to establish the roles and responsibilities they have compared to that of the organization who uses the service. Although these roles differ, both are equally crucial to ensuring the ongoing integrity and accessibility of data.

In the context of Microsoft 365, Microsoft assumes the role of service provider and is primarily responsible for ensuring the uptime of its cloud services. This is achieved through geo-redundancy across its datacenters, which minimizes service interruptions. Additionally, Microsoft offers essential safeguards like the Recycle Bin and retention policies to address basic short-term data loss recovery needs. However, the Shared Responsibility Model clearly indicates that the responsibility for access and control of data ultimately lies with the user. To effectively fulfill this responsibility, organizations must implement a robust data backup strategy for Microsoft 365, which ensures that backups are stored separately from the original data and can be easily recovered at a moment's notice. Unlike the short-term retention needs that are natively available within Microsoft 365, organizations must ensure longer term data retention needs are met and that they can access and restore data at specific points in time.

### The Microsoft 365 Shared Responsibility Model



In addition to ensuring data accessibility, organizations must also address Microsoft 365's security and regulatory requirements, which feature a distinct division of responsibilities. Microsoft is responsible for securing infrastructure-level concerns, which encompasses both the physical security of its datacenters and application-level security, which allows administrators to customize security controls as needed. Conversely, organizations must focus on data-level security measures to mitigate risks associated with internal and external data loss, including potential cyber incidents.

As a data processor, Microsoft adheres to its own data privacy and regulatory obligations, while organizations using the service assumes the role of data owners. This entails fulfilling their corporate compliance and regulatory requirements, which further emphasizes the necessity for organizations to maintain control over the management and protection of their critical data.

# Overview of Veeam Data Cloud

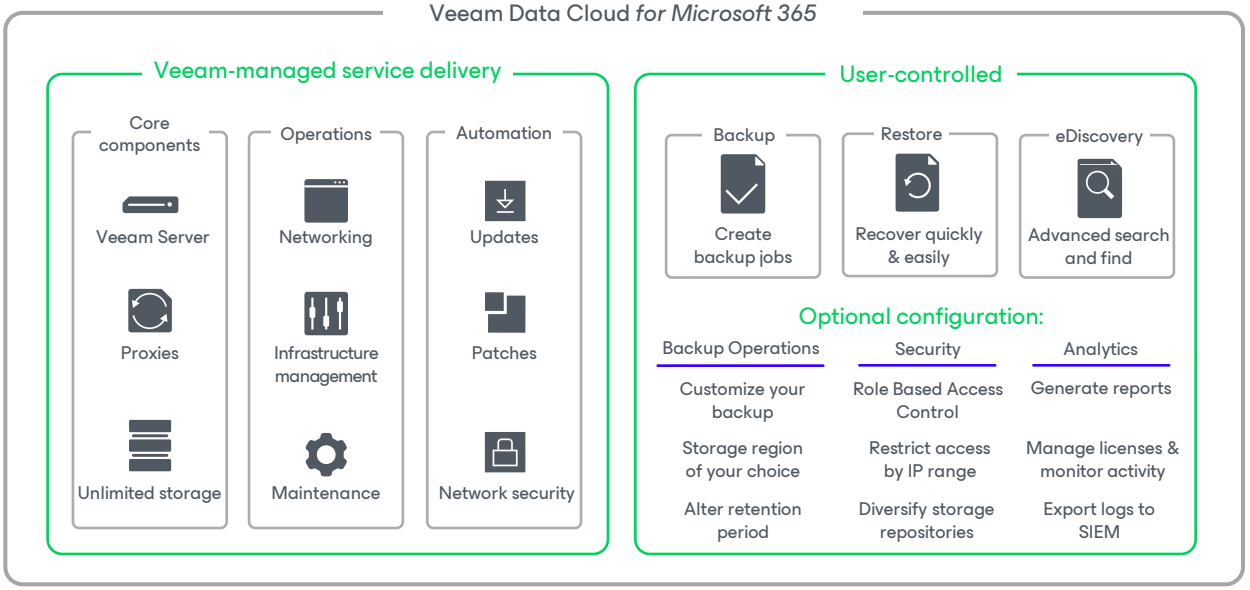
## How Veeam Offers SaaS Backup

Veeam Data Cloud *for Microsoft 365* utilizes Microsoft Entra ID applications to facilitate the backup of Microsoft 365 data. During the **self-service onboarding process**, users can choose to automatically or manually create enterprise applications and application registration in Entra ID. If opting for automatic connection, Veeam Data Cloud generates a new application registration and grants the necessary permissions. For manual connections, users must grant permissions for new or existing application registrations. Additionally, users can enhance SharePoint backup speed by adding a second Microsoft Entra ID application registration.

The backup retention mechanism employed by Veeam Data Cloud is snapshot-based and captures and stores the state of each backed-up item during each backup job. This approach allows Veeam to maintain cumulative item versions for specific restore points. The default retention period is set to seven years, but it can be customized to allow for unlimited retention upon request. Once data is backed up, it cannot be deleted, which ensures that historical data remains available for compliance and recovery purposes.

## What Comes With Veeam Data Cloud

Veeam includes many aspects in the service delivery of Veeam Data Cloud *for Microsoft 365*. This web-based backup comes with all major infrastructure components that are pre-configured for the customer. These components include the software, the backup server, backup proxies, and unlimited storage. Veeam also handles some back-end operational aspects on behalf of the customer, such as networking and implementing patches and updates. While Veeam hosts the service, the user has full control over their backup, restore, and search operations, as well as the ability to tailor user access and security restriction protocols as required.



## Backup policies

Veeam Data Cloud *for Microsoft 365* has two backup policies that come in the form of three distinct plans: Flex, Express, and Premium, each tailored to provide varying levels of data protection coverage.

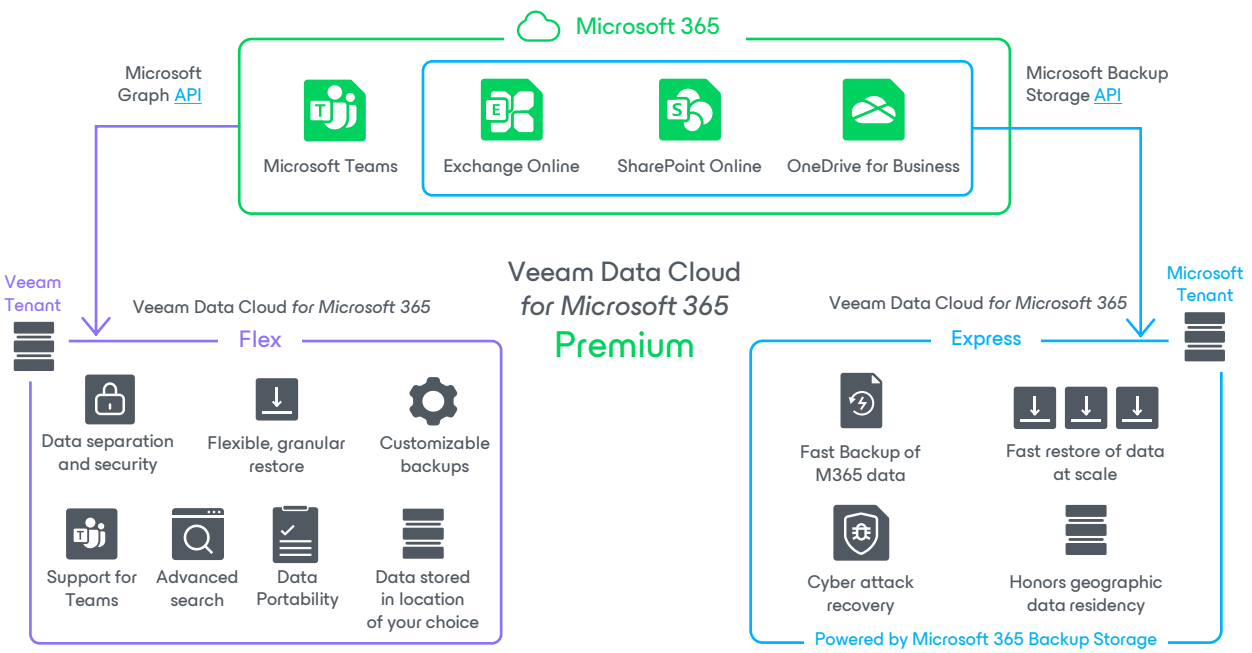
**Flex** addresses operational backup and recovery requirements by offering customizable backup and retention options, file-level granular recovery capabilities, and the ability to separate and select data locations. Unlike Express, Flex edition includes support for Microsoft Teams and emphasizes flexibility to meet both operational and compliance-driven data protection needs. This plan can be purchased as a standalone option or bundled with Entra ID protection for an additional fee.

**Express** integrates with Microsoft 365 Backup Storage, Microsoft's first-party backup solution, and is specifically designed to meet disaster recovery (DR) needs that require rapid restoration of substantial amounts of Microsoft 365 data. This solution eliminates system throttling by facilitating backup and recovery speeds of 1-3TB per hour, delivered through backup operations within the Microsoft 365 tenant.

**Premium** combines the features of both the Express and Flex solutions and allows for the management of backup policies through a single interface. This plan effectively addresses a wide range of data protection and recovery needs by leveraging the benefits of flexible operational mechanisms alongside the speed and scale of DR. Entra ID protection is included by default in the Premium plan.

While Premium is generally recommended for optimal data protection for Microsoft 365, organizations may also opt to implement Premium for key users such as C-suite executives, Finance, and R&D personnel while providing the Flex plan for their other users.

For a comprehensive overview of the differences between each plan, refer to the Plans Comparison Guide.



# Data Backup

## Flex Backup Capabilities

**Backup Frequency**
The Flex backup solution allows organizations to achieve a recovery point objective (RPO) that's as low as three times daily. By default, the backup policy runs once every 24 hours but can be configured every eight hours via support.

Veeam Data Cloud supports the execution of multiple backup jobs with varying frequencies, which enables organizations to assign different RPOs to distinct data sets. This functionality allows administrators to create numerous backup jobs within a single Microsoft 365 organization, which thereby optimizes backup strategies across diverse data types. In contrast to standard solutions that typically use a single backup schedule, Veeam's approach provides the flexibility to cater to specific data protection requirements.

**Retention Period**
The retention capabilities within Veeam's Flex backup solution are robust, which allows organizations to retain backups for extended periods. By default, backups can be retained for up to seven years. However, customers have the option to customize their retention period to a specific number of years or unlimited retention, as well as the ability to use multiple retention options. This enhances the ability to manage data in compliance with regulatory and internal policies.

## Express Backup Capabilities

**Backup Frequency**
Under the Express backup policy, backup frequency is fixed for different applications. OneDrive and SharePoint backups occur every 15 minutes for the first two weeks, after which only one backup per week is retained. Exchange data is continuously backed up as changes occur. While this ensures timely protection, it also limits flexibility, which makes it difficult for organizations to adapt backup frequencies to their specific needs.

The Express backup policy operates under a single schedule and processes all users and datasets within the same framework. This results in a uniform recovery point objective (RPO) and retention policy across the organization, thus simplifying management but restricting customization for diverse data sets or user groups. As a result, aligning backup practices with varying business requirements can be challenging.

**Retention Period**
The retention period for backups under the Express policy is fixed at one year, which prevents customers from customizing their timeframe. While users can view existing retention and backup frequency settings, these are not adjustable. This limitation may pose challenges for organizations that need longer retention durations to meet compliance or internal governance standards.

# Data Recovery

## Flex Recovery Capabilities

**Restore Options**
The Flex backup policy supports a wide range of granular restore options, which enables organizations to recover data at the file level, across users, and to alternate locations. Administrators can restore items to their original mailbox, different mailboxes, original folders, or alternative folders. This policy facilitates the recovery of modified and deleted items to ensure that users can easily access the data they need when it is required.

**Self-Service Restore Portal**
Flex includes a self-service restore portal, which allows organizations to delegate restore tasks to end-users or restore operators. This functionality empowers users to manage their own restore requests, which reduces administrative overhead. Additionally, organizations can create custom roles through extensive roles and permissions settings to ensure that users have appropriate access levels tailored to their specific responsibilities.

**Search Scope**
The Flex backup policy provides a centralized search capability that lets users effortlessly locate specific items within large volumes of backups. This feature allows for comprehensive searching across mailboxes, OneDrive, SharePoint sites, and Teams, which streamlines the recovery process and enhances productivity.

**Search Filters**
Flex offers comprehensive search filters, which allows users to refine their searches with over 60 filter fields for each service. This capability facilitates quick identification of specific items within extensive backup data, with the added ability to combine filters for more precise results. As a result, organizations can efficiently manage their data recovery processes and ensure that critical information is readily accessible.

## Express Recovery Capabilities

Under the Express policy, Exchange, SharePoint, and OneDrive for Business can be restored back to their original location. There are currently no granular restore options for SharePoint and OneDrive for Business.

Veeam Data Cloud supports bulk recovery for multiple mailboxes, SharePoint sites, and OneDrive users within a single restore job/request, which streamlines recovery for larger datasets. However, bulk recovery for Microsoft Teams data is not yet supported, thus limiting recovery options for teams that heavily use this platform.

# Data Security

## Built-In Security Measures

Veeam is dedicated to maintaining a secure, compliant, and resilient environment for customers by continually enhancing its information security and corporate compliance initiatives. These solutions encompass not only built-in security measures, but customizable access and control capabilities that enable organizations to manage backup data efficiently too. Veeam Data Cloud *for Microsoft 365* ensures data protection and privacy through a variety of mechanisms and controls:

- **Multi-factor authentication (MFA):** Implements Microsoft single sign-on combined with MFA to enhance security.
- **Data encryption:** Backup files are encrypted both at rest and in transit using AES-256 encryption, which offers robust protection against unauthorized access.
- **Immutable backups:** Provides service-level immutability for primary backups, which ensures that once data is backed up, it cannot be altered, tampered with, or deleted by users. This includes administrators or attackers.
- **Zero trust architecture:** Built on a zero-trust security model that minimizes the risk of unauthorized access by verifying every access request.
- **Data separation:** Data is stored within the Microsoft security boundary, which ensures compliance with Microsoft's security standards while enabling secure data separation.
- **Isolated environment:** Backup data is stored in a virtually air-gapped location hosted by Veeam in Microsoft Azure. This isolated environment is decoupled from both Microsoft 365 and customer infrastructure, benefiting from the inherent data security provided by Microsoft Azure at the storage level.
- **Role-based access control (RBAC):** Administrators can create user roles and assign permissions to control access and actions for users within the organization. This level of control allows admins to adhere to the principle of least-privilege.
- **Dynamic Entra ID groups:** Using dynamic Entra ID groups for user-based backup policies ensures that the backup scope automatically adjusts to changes in the user base, which thereby enhances data protection and privacy.

## Data Sovereignty

Veeam enables organizations to meet data residency requirements by allowing deployment of Veeam Data Cloud in any available Microsoft Azure region, which adheres to local compliance, security, and regulatory requirements. Selecting data centers in proximity optimizes performance and minimizes potential latency. Veeam provides full control over where backup data is stored and processed:

- **Location flexibility:** The solution allows data to be stored within the Microsoft security boundary or in a location of the customer's choosing to ensure compliance with data sovereignty laws.
- **Support for regional storage requirements**: The customizable backup configuration includes the ability to specify geographic locations for data storage, which is essential for meeting local regulatory requirements.

## GDPR Compliance

Veeam Data Cloud *for Microsoft 365* can support GDPR strategies by providing features which support data subject rights, data breach notifications, and data transfer mechanisms. Veeam Data Cloud *for Microsoft 365* can help organizations comply with GDPR requirements in several ways:

- **Retention period:** Retention is set to seven years by default and can be customized to offer unlimited time.
- **Data subject rights:** Supports granular restore and data export options to allow administrators to respond efficiently to data subject access requests.
- **Data transfer mechanisms:** Backups can be stored in the geographical location of your choice, which ensures compliance with GDPR data transfer and data sovereignty requirements.
- **Customizable retention policies:** Veeam Data Cloud *for Microsoft 365* allows you to set customizable retention periods across different repositories. Aligning these retention settings with your organization's data retention policies ensures compliance with GDPR requirements.

## Data Discovery for Legal Requests

Veeam Data Cloud *for Microsoft 365* supports data discovery workflows, including how data can be searched, retrieved, and preserved in response to legal requests or investigations. It supports robust eDiscovery capabilities in the following ways:

- **Advanced search and granular recovery:** The solution includes advanced search features that allow administrators to quickly find and retrieve specific data needed for legal requests or investigations.
- **Data preservation:** Granular recovery and export options facilitate the preservation of relevant data, which supports legal hold requirements and regulatory compliance.

## Audit Trails and Reporting

Veeam offers comprehensive audit and reporting capabilities to ensure that data can be reported on and managed for record keeping requirements.

- **Automated detailed reporting:** Veeam Data Cloud *for Microsoft 365* provides comprehensive audit trails and reporting features, including preconfigured dashboards and reports for compliance auditing and regulatory needs.
- **Event monitoring and notifications:** Veeam Data Cloud *for Microsoft 365* can capture session and user logging which can be viewed in reports, or notifications via email recipients for Veeam Data Cloud system notifications. Monitoring with common security platforms can also be done by defining a syslog server where you can receive Veeam Data Cloud user activity logs.

To read more about security capabilities in Microsoft 365, read 10 Steps to Microsoft 365 Cyber Resilience.

# Global Security Certifications

Veeam upholds the highest standards of security by implementing a robust security certification program that ensures the availability, integrity, and confidentiality of customer data. This program ensures that Veeam Data Cloud and other Veeam solutions also adhere to relevant industry, governmental, and international standards, which reflects Veeam's dedication to best practices in cybersecurity and regulatory compliance.

**SOC 2 Type 2** assesses an organization's internal control design and operational effectiveness to evaluate compliance with the Trust Services Criteria, which encompass security, availability, processing integrity, confidentiality, and privacy. This assessment ensures that the controls in place function as intended over a specified period, thereby demonstrating the organization's commitment to maintaining a secure and compliant environment.

Veeam fulfills **SOC 2 Type 2 requirements** by implementing a comprehensive security and compliance program that adheres to industry best practices. This program includes stringent access controls, continuous monitoring, data encryption, and effective incident response protocols, which are all designed to safeguard data and ensure compliance.

**The International Organization for Standardization (ISO)** is a globally recognized entity that establishes best practices across various industries, including information security, cybersecurity, quality management, and data protection. Through the development of standardized frameworks, ISO empowers organizations to implement structured and effective security programs that comply with industry regulations and legal requirements. These standards serve as a foundation for maintaining data integrity, confidentiality, and availability, while also ensuring operational resilience in an ever-evolving threat landscape.

Veeam adheres to key **ISO standards**, seamlessly integrating them into its security and compliance framework to enhance data protection and mitigate risk. These include:

- ISO 27001 — Information Security Management Systems (ISMS)
- ISO 27017 — Cloud Security
- ISO 27018 — Data Privacy in Cloud Computing
- ISO 27701 — Privacy Security
- ISO 22301 — Business Continuity
- ISO 9001 — Quality Management

**The Health Insurance Portability and Accountability Act (HIPAA)** and the Health Information Technology for Economic and Clinical Health Act (HITECH) establish essential security, privacy, and breach notification requirements for organizations that handle protected health information (PHI). A HIPAA/HITECH Type 2 Attestation involves an independent third-party assessment that evaluates an organization's compliance with these regulatory frameworks over a specified period, ensuring that appropriate administrative, physical, and technical safeguards are in place to protect sensitive healthcare data.

Veeam has achieved **HIPAA and HITECH** compliance by implementing a comprehensive data protection strategy designed specifically to safeguard PHI. By employing advanced encryption, stringent access controls, event monitoring, and robust data integrity mechanisms, Veeam enables healthcare organizations to meet the rigorous security and privacy standards mandated by these regulations.

Veeam has a roadmap which ensures that Veeam Data Cloud will acquire additional certifications not listed. We are transparent about all our certifications, and the full list of official certification records can be accessed on our **Compliance Portal**.

# Key Difference Makers

**Veeam offers unique benefits for Microsoft 365 data protection that the general competition does not match.**

### Safest Investment
Invest in Veeam for peace of mind, as Veeam is the #1 and most proven Microsoft 365 backup solution that's battle tested by 23.5+ million users (800+ Microsoft 365 user reviews for an average 4.5/5 on product review platforms).

### Speed and Control
Get speed, scale, data resilience, and flexibility with Veeam Data Cloud Premium, which combines Veeam Data Cloud and Microsoft 365 Backup Storage in a single platform. Veeam keeps licensing costs low and predictable with a fixed price per user, no matter the amount of data.

### Higher Productivity
Reduce backup administrators' workload by shortening or automating manual tasks with capabilities like advanced search and bulk recovery, and by delegating tasks to end-users with a self-service restore portal and to IT operators with customizable RBAC.

### Microsoft 365 + Entra ID
Protect Microsoft 365 and Entra ID with a single platform for simplicity. It is especially useful as Entra ID complements Microsoft 365 in some data recovery scenarios. Lower costs by bundling Entra ID with Microsoft 365 backup, so that you only license Microsoft 365 users, not all Entra ID users.

### Data Sovereignty
Store backups in any cloud region around the world to optimize performance or adhere to local compliance, security, and regulatory requirements, or change location over time to adapt to your evolving IT strategy. Technical support is needed in some scenarios.

### Exit Strategy
Avoid vendor lock-in and protect your investment in backup, as you may retain your backups if you end your Veeam subscription and may use Veeam's free powerful search and recovery tool to recover your backup data to Microsoft 365 afterwards.

### Cost Control
Avoid unplanned costs as data grows and hidden fees for major capabilities like advanced search, as Veeam's license includes unlimited storage and all capabilities at a fixed price per user.

### Reduced Data Loss
Minimize data loss by running backups as often as three times per day for an RPO of eight hours.

## About Veeam Software

Veeam®, the #1 global market leader in data resilience, believes every business should be able to bounce forward after a disruption with the confidence and control of all their data whenever and wherever they need it. Veeam calls this radical resilience, and we're obsessed with creating innovative ways to help our customers achieve it. Veeam solutions are purpose-built for powering data resilience by providing data backup, data recovery, data portability, data security, and data intelligence. With Veeam, IT and security leaders rest easy knowing that their apps and data are protected and always available across their cloud, virtual, physical, SaaS, and Kubernetes environments. Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 67% of the Global 2000, that trust Veeam to keep their businesses running. Radical resilience starts with Veeam. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.

→ Learn more: www.veeam.com