Leitfaden zur #1 Backup-Lösung für Microsoft 365 von Veeam

Technische Hinweise zu
Veeam Backup *for Microsoft 365*

Michele Domanico,
Edward Watson

veeam.com/de

Inhalt

Der Markt für Microsoft 365-Datensicherungslösungen

Bei der Sicherung von Microsoft 365-Daten hat sich in den letzten vier bis fünf Jahren viel getan. Unsere Umfragen zwischen 2017 und 2019 hatten ergeben, dass sich die meisten Nutzer allein auf die nativen Tools von Microsoft verließen. Nur ein sehr geringer Prozentsatz der Umfrageteilnehmer gab an, Microsoft 365-Daten überhaupt nicht zu sichern.

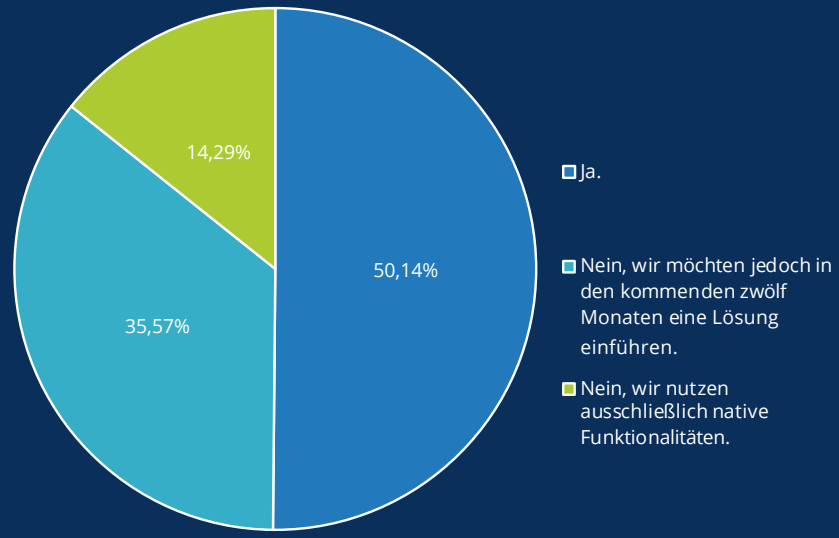
2019 wendete sich das Blatt. Nur noch 20 % der Befragten verwendeten ausschließlich die Tools in Microsoft 365, während der Anteil der Nutzer, die Microsoft 365-Daten überhaupt nicht sichern, auf 47 % gestiegen war.

Diese deutliche Zunahme lässt sich dadurch erklären, dass Unternehmen, die ihre Daten mit den Tools von Microsoft bislang für ausreichend geschützt hielten, nach und nach erkannten, dass diese nativen Funktionalitäten nicht mit einer Backup-Lösung vergleichbar sind. Ihnen ist heute bewusst, dass ihre Datensicherung lückenhaft ist. Durch die Einführung von Backup-Lösungen von Drittanbietern möchten sie einen zuverlässigen Schutz ihrer Daten gewährleisten.

Der Trend, sich nicht mehr ausschließlich auf native Funktionalitäten zu verlassen, hält an. Laut IDC setzen 14 % der Unternehmen ausschließlich native Funktionalitäten ein. 35 % haben vor, in den nächsten zwölf Monaten eine SaaS-Lösung für die Datensicherung einzuführen.

Benötigen Sie noch weitere Argumente? Im Blog-Beitrag unter https://www.veeam.com/blog/de/office365-shared-responsibility-model.html

Q. Verfolgt Ihr Unternehmen spezielle Strategien für die Sicherung und Wiederherstellung von Daten in SaaS-Umgebungen?



IDC

Quelle: IDC CloudOps Survey, 2023

Planung Ihrer Microsoft 365-Datensicherung

- Installationspaket
- Infrastrukturkomponenten
- Einfache und erweiterte Bereitstellungen
- Infrastrukturplanung
- Bereitstellungsoptionen
- Unterstützter Storage
- Aufbewahrungsrichtlinien
- Backup-Architektur

Installationspaket

Das Image für die Installation von Veeam® Backup *for Microsoft 365* umfasst die folgenden Komponenten:

1. Veeam Backup *for Microsoft 365*

Installiert Veeam Backup *for Microsoft 365* zusammen mit diesen Services:

- einem Server für die Steuerung der globalen Konfigurationseinstellungen und das Management
- einer Konsole mit der Client-Benutzeroberfläche
- einem RESTful API-Plug-in und einem Wiederherstellungsportal (diese Komponente ist standardmäßig deaktiviert, kann jedoch aktiviert werden)
- einer PowerShell-Erweiterung zur Automatisierung von Abläufen
- Veeam Explorers™ zur Wiederherstellung gesicherter Daten

2. Veeam Backup *for Microsoft 365*-Konsole

Installiert diese Services:

- Client-Benutzeroberfläche für lokale und Remote-Server mit Veeam Backup *for Microsoft 365*
- Veeam Explorers für die Datenwiederherstellung

3. Veeam Backup *for Microsoft 365*-PowerShell

Installiert die PowerShell-Erweiterung mit verschiedenen PowerShell-Cmdlets.

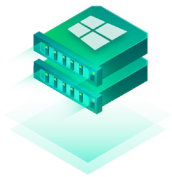
4. RESTful API und Wiederherstellungsportal für Veeam Backup *for Microsoft 365*

Installiert das RESTful API-Plug-in und das Wiederherstellungsportal.

Das Installationspaket für Veeam Backup *for Microsoft 365* steht auf der offiziellen Veeam-Website zum Download bereit.

Infrastrukturkomponenten

Veeam Backup *for Microsoft 365* ist eine umfassende Lösung für die Sicherung und Wiederherstellung Ihrer Microsoft 365-Daten beispielsweise in Microsoft Exchange, Microsoft SharePoint, Microsoft OneDrive for Business und Microsoft Teams. Auch Daten aus lokalen Microsoft Exchange- und SharePoint-Umgebungen lassen sich damit sichern und wiederherstellen. Diese **Lösung umfasst drei Kernkomponenten**: Backup-Server, Backup-Proxy und Backup-Repository.Sie beinhaltet außerdem ein RESTful API-Plug-in und PowerShell.



Backup-Server

Der Veeam Backup *for Microsoft 365*-Server ist die zentrale Konfigurations- und Steuerungskomponente. Über diesen Server werden z. B. andere Komponenten eingerichtet und verwaltet, Jobs geplant und Aufgaben koordiniert.

Er kann auf einem physischen oder virtuellen Windows-System installiert werden. Über den Server ist der Zugriff auf die Benutzeroberfläche der Konsole möglich.

Backup-Proxy

Der Veeam Backup *for Microsoft 365*-Proxy führt im Hintergrund sämtliche Lese- und Schreibvorgänge aus und wandelt Objekte auf intelligente Weise in kleinere Elemente um, die sich einfacher verwalten lassen.

Er stellt eine optimale Route für den Backup-Traffic bereit und ermöglicht eine effiziente Datenübertragung.

Backup-Repository

Im Veeam Backup *for Microsoft 365*-Repository werden die Microsoft 365-Daten gespeichert. Repositorys können auch wichtige Metadaten speichern, die bei Sicherungs- und Wiederherstellungsvorgängen verwendet werden.

Backup-Repositorys werden auf den folgenden Storage-Typen unterstützt: lokaler und cloudbasierter Objektspeicher, Direct Attached Storage (DAS), SAN und SMB (Server Message Block 3.0).

Einfache und erweiterte Bereitstellungen

Veeam Backup *for Microsoft 365* unterstützt sowohl einfache als auch erweiterte Bereitstellungen. Wählen Sie die Bereitstellungsmethode, die Ihren Anforderungen am besten entspricht.

Einfache Bereitstellungen

Bei der einfachen Bereitstellung werden alle Komponenten auf einem Server installiert. Dabei kann es sich um eine virtuelle oder physische Maschine handeln. Die Spezifikationen sollten der Maximalkonfiguration entsprechen. Bei diesem Szenario werden alle wesentlichen Komponenten (Server, Proxy und Repository) auf demselben System installiert.

Um eine einfache Bereitstellung zu skalieren, können Sie weitere Repositorys hinzufügen, die über denselben integrierten Proxy-Server betrieben werden. Einfache Bereitstellungen eignen sich für KMU, die Backup-Kopien ihrer Microsoft 365-Daten in der lokalen Umgebung speichern möchten. Dies gilt auch für Public-Cloud-Umgebungen wie Azure und AWS sowie für weitere Cloud-Angebote. In diesem Fall können Backup-Daten in festplatten-/dateibasierten Repositorys gespeichert werden, die mit den Servern verbunden sind, sowie in Objektspeicher-Repositorys in der Public Cloud und lokalen Umgebungen.

Erweiterte Bereitstellungen

Die erweiterte Bereitstellung ermöglicht die Skalierung von Installationen durch zusätzliche Proxy- und Repository-Komponenten, um auch anspruchsvollen Anforderungen gerecht zu werden. Diese Komponenten werden über den zentralen Server hinzugefügt. Dabei werden die erforderlichen Komponenten auf den jeweiligen Servern installiert, indem der zentrale Service Veeam.Archiver.Proxy zusammen mit einer Kopie der Infrastrukturkonfiguration auf diesen bereitgestellt wird.

Über diesen neu hinzugefügten Proxy haben Sie die gesamte Infrastruktur im Blick und können Backup-Jobs für zusätzliche Repository-Ziele konfigurieren. Sie werden bei allen Schritten von einem Assistenten unterstützt. Mit den nativen PowerShell-Befehlen und RESTful APIs lassen sich außerdem sämtliche Prozesse automatisieren. Server und Proxys können derselben Domäne angehören, sich in unterschiedlichen Domänen (mit einer Vertrauensbeziehung) befinden oder auch Teil von Arbeitsgruppen sein.

Infrastrukturplanung

In der Regel orientiert sich das Bereitstellungsmodell an der Größe einer Umgebung. Die Größe einer Umgebung definiert sich nicht notwendigerweise nach der Anzahl der zu schützenden Microsoft Office 365-Nutzer, sondern basiert vielmehr auf der Anzahl der zu schützenden Objekte. Folgende Objekte werden unterstützt:

Microsoft Exchange

- Primäre Postfächer
- Archivpostfächer
- Freigegebene Postfächer
- Öffentliche Ordner
- Ressourcenpostfächer

Microsoft SharePoint

- Websites für die Zusammenarbeit
- Kommunikationswebsites
- Persönliche Websites

Microsoft OneDrive for Business

- OneDrive for Business-Konten

Microsoft Teams

- (einschließlich Kanäle und Registerkarten)

Empfohlene Maximalkonfigurationen

Max. Anzahl von Objekten pro Instanz	Max. Anzahl von Objekten pro Proxy	Max. Anzahl von Benutzern pro Job	Max. Anzahl von Proxys pro Bereitstellung	Max. Anzahl von Benutzern pro Proxy	Max. Anzahl von Benutzern pro Bereitstellung	CPU/ RAM pro Proxy	Max. Größe pro Repository
1.000.000	20.000	5.000	50	5.000	250.000	8 CPUs/32 GB	Unbegrenzt

Unkomplizierte Dimensionierung: Nutzen Sie den Veeam Backup *for Microsoft 365*-Kapazitätsrechner, um Ihre Umgebung zu dimensionieren!

Bereitstellungsoptionen

Ihre Bereitstellung von Veeam Backup *for Microsoft 365* kann in lokalen, Privat-Cloud-, Public-Cloud- und Hybrid-Cloud-Umgebungen ausgeführt werden. Die Voraussetzungen und die Funktionsweise der Komponenten in den verschiedenen Umgebungen sind sehr ähnlich. IT-Organisationen können unter verschiedenen Designs wählen, um ihre jeweiligen Anforderungen zu unterstützen.

Lokale Bereitstellungen

Eine lokale Bereitstellung ist die beste Option für Kunden, die eine Backup-Kopie ihrer Microsoft 365-Daten in der lokalen Umgebung speichern möchten, da sie sich unkompliziert auf eine erweiterte Bereitstellung skalieren lässt. Diese Bereitstellungsoption bietet Unternehmen mit hybriden Microsoft 365-Umgebungen, in denen die geschützten Daten online und/oder in der lokalen Infrastruktur gespeichert werden, die nötige Flexibilität.

Bereitstellung über Serviceprovider

Veeam Backup *for Microsoft 365* wird von Serviceprovidern eingesetzt, die BaaS für Microsoft 365-Daten anbieten. Diese Infrastruktur ist flexibel und kann für den „exklusiven" Zugriff auf einzelne Mandanten und in einem „gemeinsam genutzten Modus" mit Mandantenfähigkeit verwendet werden, bei dem mit demselben Service mehrere, auf unterschiedliche Repositorys verteilte Unternehmen unterstützt werden können.

Bereitstellungen in Azure und AWS

Für die Bereitstellung in Microsoft Azure steht über den Azure Marketplace eine zertifizierte und vorinstallierte Anwendung zur Verfügung. Kunden müssen dabei die Details ihrer Microsoft 365-Mandanten im Azure Marketplace eingeben. Auch für die Bereitstellung in AWS steht über den AWS Marketplace eine zertifizierte Anwendung zur Verfügung, die auf einer AWS EC2-Instanz vorinstalliert ist. Sie müssen lediglich den Instanztyp auswählen, der Ihren Anforderungen am besten entspricht.

Sonstige Public-Cloud-Provider

Veeam Backup *for Microsoft 365* kann auch in den Umgebungen anderer Cloud-Provider Ihrer Wahl bereitgestellt werden. Die Ausführung von Veeam Backup *for Microsoft 365* ist prinzipiell in jeder Cloud möglich. Sofern die Mindestanforderungen für die Bereitstellung erfüllt sind, können Sie einen beliebigen Public-Cloud-Provider wählen. Dabei haben Sie dennoch die Möglichkeit, Daten bei Bedarf an einem separaten Ort zu speichern.

Unterstützter Storage

Veeam Backup *for Microsoft 365* unterstützt verschiedene Speicheroptionen. Backup-Repositorys werden auf folgenden Storage-Typen unterstützt:

Objektspeicher

Unternehmen mit einer Cloud-First-Strategie können ihre Veeam-Backups auf Objektspeicher ablegen. Unterstützt werden unter anderem AWS S3, Microsoft Azure Blob Storage, die IBM Cloud sowie S3-kompatibler Storage in der Cloud und in lokalen Umgebungen. Sie können auch Backup-Kopien (mit aktivierter Immutability) auf Objektspeicher ablegen, beispielsweise auf Amazon S3, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive, Azure Blob oder Azure Archive.

DAS

Ebenfalls unterstützt wird Direct Attached Storage (DAS), unter anderem USB/eSATA und Raw Device Mapping (RDM).

SAN

Über Hardware, einen virtuellen Host-Busadapter (HBA) oder iSCSI-Initiatoren können der Server und der Proxy mit einer SAN-Fabric (Storage Area Network) verbunden werden. Dadurch ist ein direkter Zugriff auf das Repository möglich. Bei einfachen Bereitstellungen steht das SAN über den Server zur Verfügung, bei erweiterten Bereitstellungen kann direkt über den Proxy auf den SAN-Storage zugegriffen werden. Der direkte Zugriff über den Proxy ist insbesondere dann von Vorteil, wenn die Ausführung von Jobs in größeren Umgebungen an Proxys delegiert wird.

Aufbewahrungsrichtlinien

Die Aufbewahrungsrichtlinie ist eine Konfiguration, die direkt auf Repositorys angewendet wird. Die globale Einstellung gilt für alle Backup-Jobs, die das entsprechende Repository verwenden. Es gibt Aufbewahrungsrichtlinien auf Objektebene und Snapshot-basierte Aufbewahrungsrichtlinien.

Aufbewahrungsrichtlinien auf **Objektebene** wirken sich auf zweierlei Weise aus:

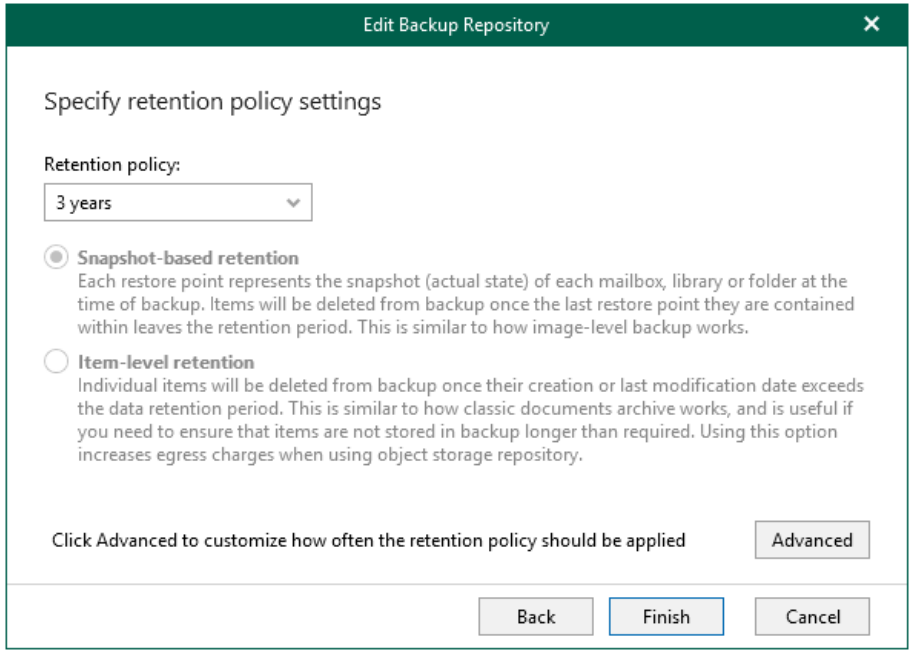
1. Beim ersten Backup wird überprüft, wann die in der Aufbewahrungsrichtlinie enthaltenen Objekte zuletzt geändert wurden. Wenn Sie beispielsweise eine Aufbewahrungsrichtlinie von drei Jahren definiert haben, beinhaltet der Backup-Job automatisch alle Objekte, die maximal drei Jahre alt sind. Objekte, die älter als drei Jahre sind, werden nicht gesichert.

2. Abhängig vom Alter der Daten und dem Datum der letzten Änderung werden alle Daten, die älter als drei Jahre sind, automatisch aus dem Repository gelöscht. Das Repository enthält zu jedem Zeitpunkt ein rollierendes Zeitfenster, das auf der Aufbewahrungsrichtlinie für den jeweiligen Zeitpunkt basiert.

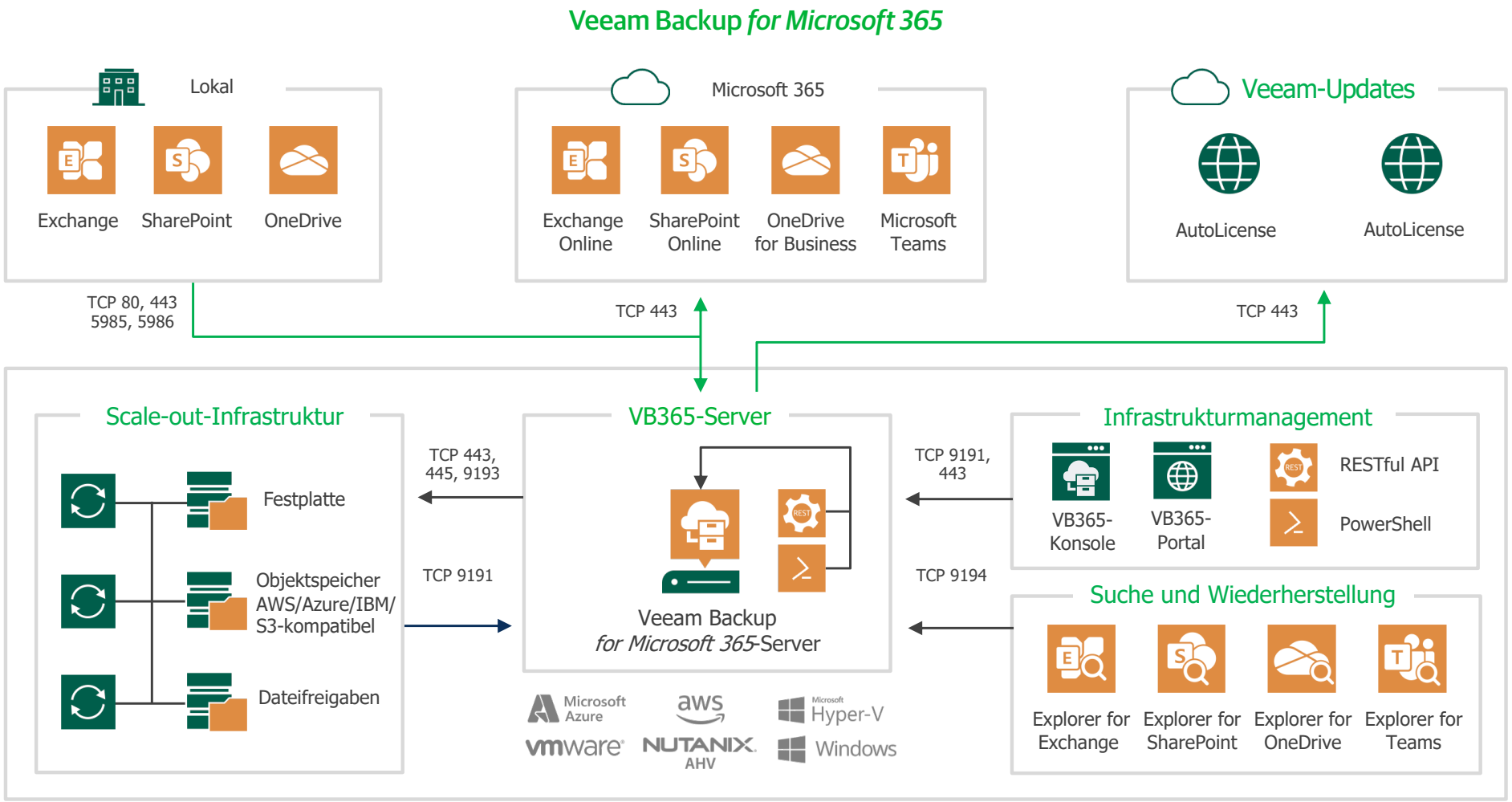
Snapshot-basierte Aufbewahrungsrichtlinien wirken sich ebenfalls auf zweierlei Weise aus:

1. Beim ersten Backup werden alle Objekte unabhängig vom Zeitpunkt ihrer Erstellung, Löschung oder Änderung in einem Full Backup gesichert. Anschließend werden Incremental Backups durchgeführt, die nur noch die seit dem letzten Backup-Job vorgenommenen Änderungen enthalten (z. B. neue, gelöschte und aktualisierte Objekte).

2. Abhängig vom Backup-Plan und dem Zeitpunkt des letzten Backups wird die Aufbewahrungsrichtlinie dann in bestimmten Intervallen auf das Repository angewendet. Damit ist die spätere Wiederherstellung auf einen bestimmten Zeitpunkt möglich.



Backup-Architektur



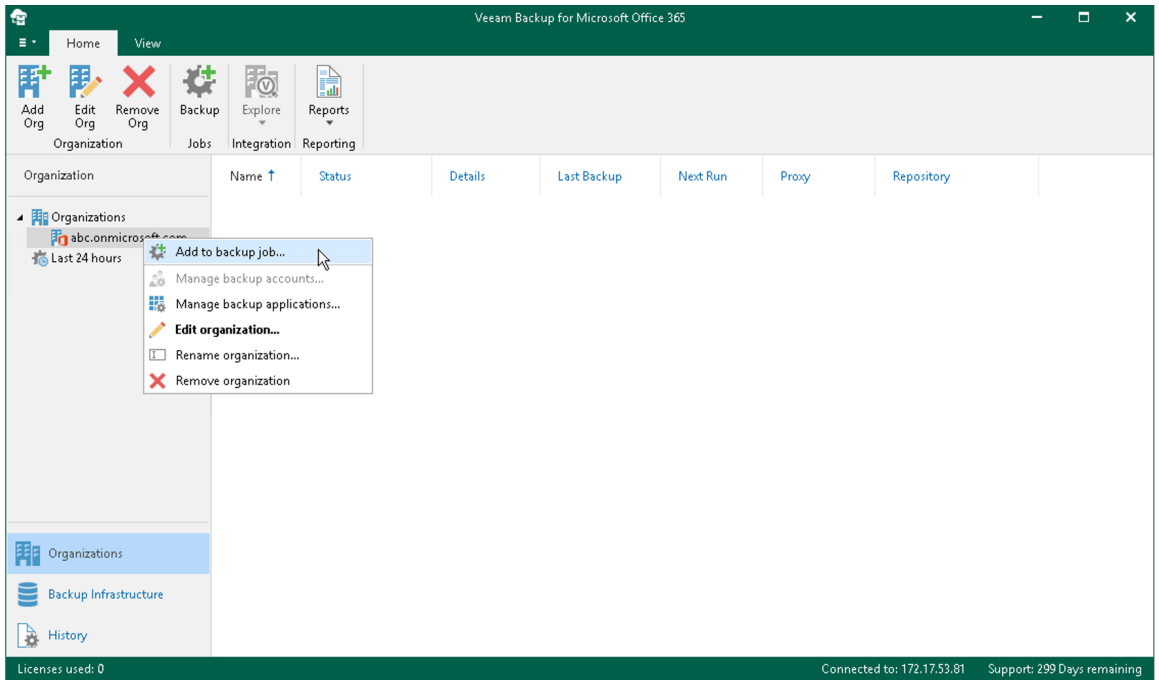
Datensicherung und -wiederherstellung mit Veeam

- Erstellung von Backup-Jobs
- Festlegung des Backup-Umfangs
- Planungsoptionen
- Veeam Explorers
- Durchsuchen von Microsoft 365-Daten
- Wiederherstellung in drei Schritten

Erstellung von Backup-Jobs

Daten in Ihren Microsoft 365- und lokalen Umgebungen werden mit Backup-Jobs gesichert.

Ein Backup-Job besteht aus verschiedenen Konfigurationparametern, mit denen eine Liste von Benutzern, Gruppen, Websites, Teams und Organisationen definiert wird, die gesichert werden sollen. Sie legen außerdem fest, wo diese Backups gespeichert werden sollen und wann neue Backups erstellt werden müssen.



Schritte eines Backup-Jobs

In Veeam Backup *for Microsoft 365* können Backup-Jobs unkompliziert mit einem Assistenten erstellt werden. Die Einrichtung von Backup-Jobs umfasst sechs Schritte:

1. Start des Assistenten für neue Backup-Jobs
2. Eingabe eines Namens für den Backup-Job
3. Auswahl der zu sichernden Objekte
4. Auswahl der auszuschließenden Objekte
5. Festlegung von Backup-Proxy und Repository
6. Definition von Planungsoptionen

Festlegung des Backup-Umfangs

In Veeam Backup *for Microsoft 365* können Sie **die gesamte Organisation oder einzelne Benutzer, Gruppen, Websites, Teams und Organisationen sichern**. Sie können außerdem festlegen, dass bestimmte Objekte nicht gesichert werden sollen. Diese Optionen stehen zur Verfügung:

Umfang festlegen

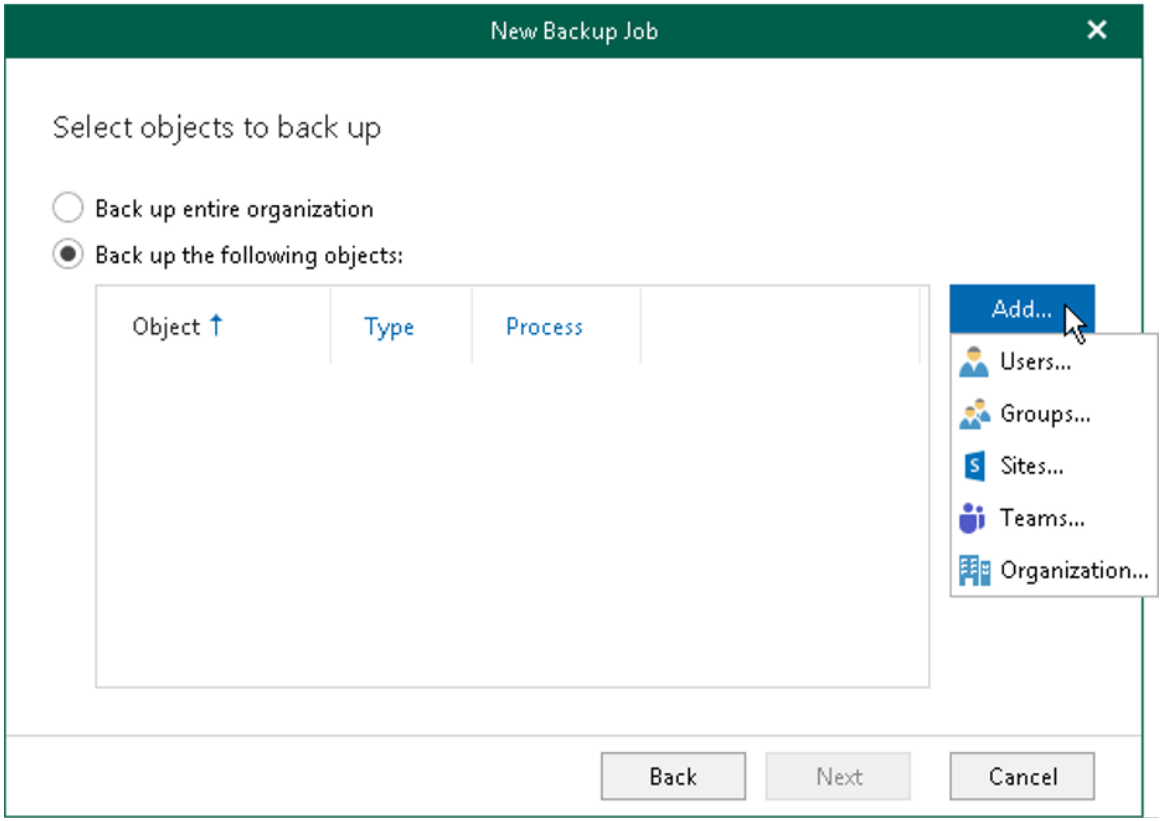
- Sicherung der gesamten Organisation.
- Sicherung einzelner Teams, Benutzer und Websites.
- Dynamische Sicherung mit Verteiler-, Sicherheits- und Microsoft 365-Gruppen.

Objekte ausschließen

- Ausschluss bestimmter Websites, Teams oder Benutzer.
- Dynamischer Ausschluss mit Verteiler-, Sicherheits- und Microsoft 365-Gruppen.

Wichtige Aspekte:

- Sie können pro Organisation nur einen Backup-Job für die gesamte Organisation erstellen.
- Objekte, die bereits mit anderen Backup-Jobs gesichert werden, sind in der Liste zur Sicherung der gesamten Organisation nicht mehr enthalten.
- Wenn Sie eine Organisation als zu sicherndes Objekt hinzufügen, werden die Verarbeitungsoptionen auf alle Benutzer, Gruppen und Websites in der ausgewählten Organisation angewendet.



Planungsoptionen

Mit Veeam Backup *for Microsoft 365* können Sie Ihre Backups genau an Ihren Anforderungen ausrichten. Diese Optionen stehen zur Auswahl:

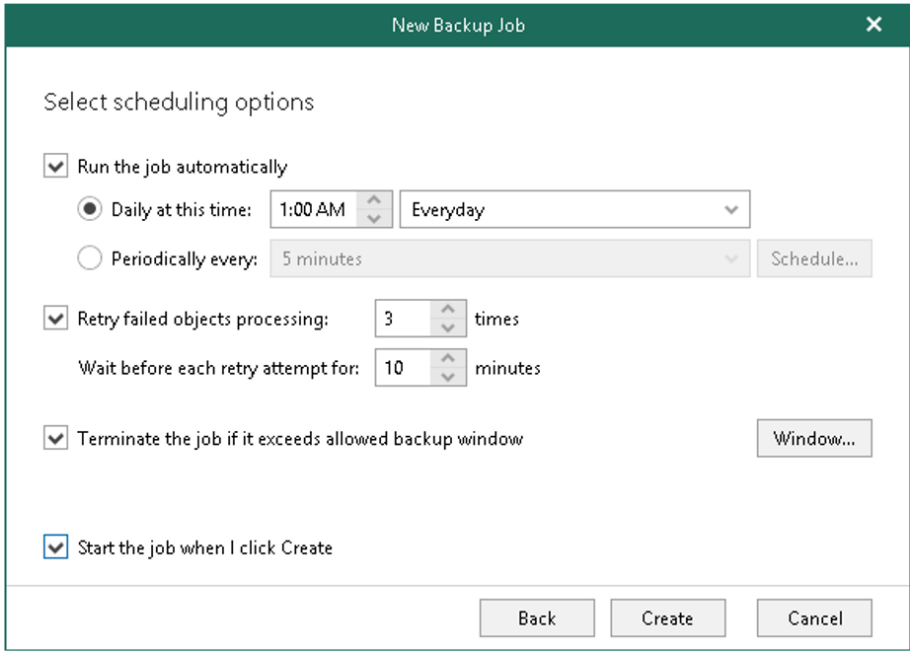
- **Daily at this time** (Täglich zu dieser Zeit): Wählen Sie diese Option, wenn der Job täglich zur angegebenen Zeit ausgeführt werden soll.
- **Periodically every (Regelmäßig alle):** Wählen Sie diese Option, wenn der Job alle **N Minuten** ausgeführt werden soll.

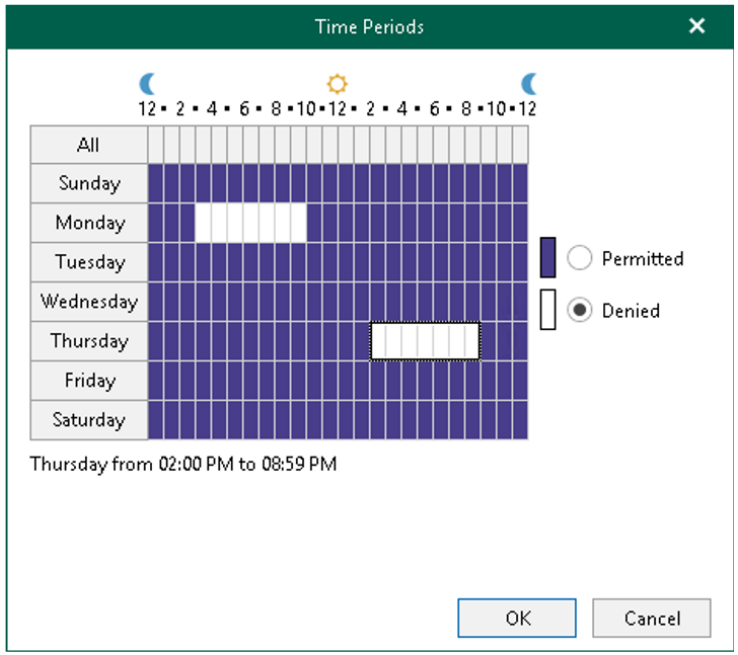
Sie können die Zeiträume auf zweierlei Weise definieren:

- Mit der Option **Permitted** (Zulässig) legen Sie fest, dass der Backup-Job im angegebenen Zeitraum ausgeführt werden kann.
- Mit der Option **Denied** (Nicht zulässig) legen Sie fest, dass der Backup-Job im angegebenen Zeitraum nicht ausgeführt werden darf.

Das Beispiel unten zeigt eine Konfiguration, bei der in diesen Zeiträumen keine Backups durchgeführt werden dürfen:

- Montags von 3:00 bis 9:59 Uhr
- Donnerstags von 14:00 bis 20:59 Uhr

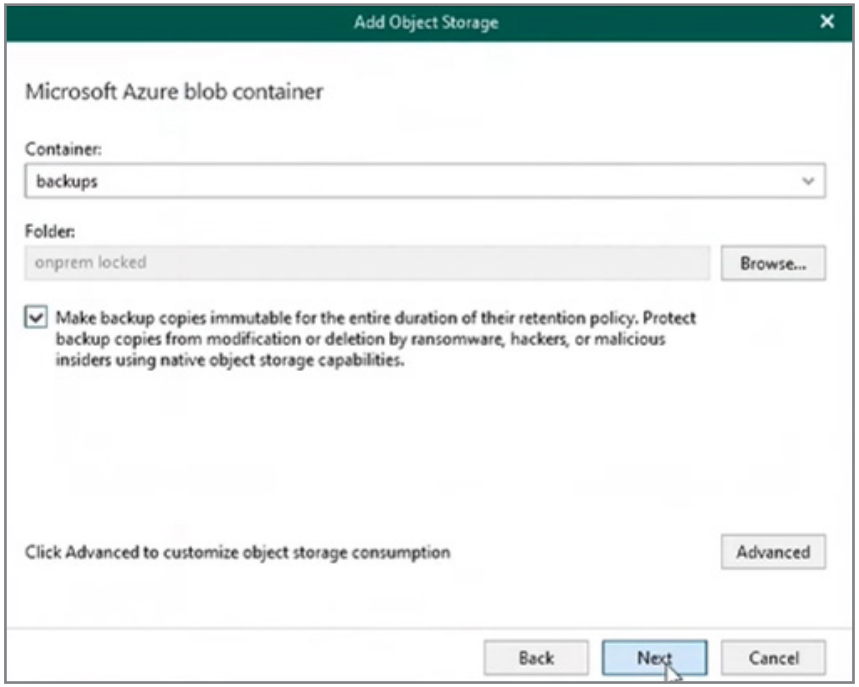




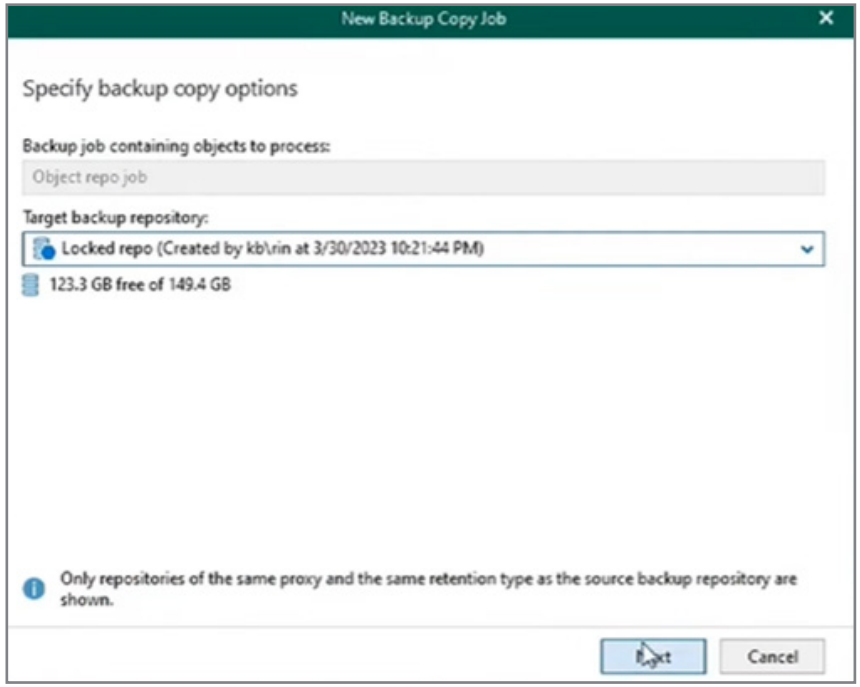
Erstellung von Backup-Kopien

Zusätzlich zu Ihrem primären Backup können Sie eine Backup-Kopie erstellen und diese mit aktivierter Immutability auf beliebigem Objektspeicher ablegen, um Ihre Daten vor Ransomware und anderen Cyberbedrohungen zu schützen. Veeam Backup *for Microsoft 365* gewährleistet die Immutability von Objektspeicher-Repositorys durch die Objektsperre und die Versionskontrolle.

- Wählen Sie „Add storage" (Storage hinzufügen), um ein gesperrtes Repository hinzuzufügen.
- Wählen Sie anschließend den Objektspeichertyp sowie das Konto und den Container des gesperrten Storage aus.
- Aktivieren Sie das Kontrollkästchen, um Ihre Backup-Kopien immutable zu machen.
- Verknüpfen Sie den Objektspeicher mit einem Backup-Repository und wählen Sie den lokalen Cache aus.



- Eine Backup-Kopie können Sie während der Erstellung Ihres primären Backup-Jobs anlegen oder indem Sie mit der rechten Maustaste auf den primären Backup-Job klicken und „Add to backup copy job" (Zu Backup-Copy-Job hinzufügen) wählen.
- Senden Sie die Kopie an das zuvor festgelegte gesperrte Repository.
- Für Backup-Copy-Jobs gibt es wie für Primary Backups verschiedene Planungsoptionen (sofortige, tägliche oder regelmäßige Ausführung).



Hinweis: Die Dauer der Sperre Ihres Backup-Copy-Repositorys entspricht Ihrem Aufbewahrungszeitraum. Diese Einstellung kann nicht nachträglich geändert werden.

Veeam Explorers

Mit den Veeam Explorers *for Microsoft Exchange*, *Microsoft SharePoint*, *OneDrive for Business* und *Microsoft Teams* können Sie Daten in Microsoft 365-, lokalen und hybriden Bereitstellungen suchen und wiederherstellen. Insgesamt stehen 50 Wiederherstellungsoptionen zur Verfügung.

Veeam Explorer *for Microsoft Exchange*

Suche und Wiederherstellung von Microsoft Exchange-Postfächern, -Ordnern, -Nachrichten, -Aufgaben, -Kontakten und -Elementen

Veeam Explorer *for Microsoft SharePoint*

Suche und Wiederherstellung von Microsoft SharePoint-Websites, -Bibliotheken und -Elementen

Veeam Explorer *for Microsoft OneDrive for Business*

Suche und Wiederherstellung von Microsoft OneDrive for Business-Objekten und -Ordnern

Veeam Explorer *for Microsoft Teams*

Suche und Wiederherstellung von Microsoft Teams-Kanälen, -Registerkarten, -Beiträgen und -Dateien

Veeam Explorers unterstützen die Backup-Architektur mit folgenden Aufgaben und Anwendungsfällen:

- **Direkte und indirekte Wiederherstellung:** Standardmäßig werden Daten an den ursprünglichen Speicherort wiederhergestellt. Dies wird als direkte Wiederherstellung bezeichnet. Bei Bedarf lassen sich Daten auch an einen anderen Ort wiederherstellen. In diesem Fall wird eine indirekte Wiederherstellung durchgeführt.
- **Durchsuchen von Inhalten:** Wenn (Online- und lokale) Microsoft 365-Daten in einem Repository gespeichert sind, ruft der Veeam Explorer diese Backup-Dateien direkt ab und stellt alle Inhalte in einem hierarchischen Format zur Verfügung. Die integrierten Browser stellen kontextbezogene Optionen bereit, mit denen die einzelnen Objekte gesendet, wiederhergestellt und exportiert werden können.
- **Suche nach Inhalten:** Die Veeam Explorers bieten eine erweiterte Suchfunktion, die ein differenziertes e-Discovery nach bestimmten Kriterien auf der Grundlage von Daten und Metadaten ermöglichen. Es stehen verschiedene Feldergruppen zur Auswahl. Für die Suche können mehrere Kriterien verwendet werden.

Durchsuchen von Microsoft 365-Daten

Sie können Microsoft 365-Daten auf vier verschiedene Arten durchsuchen:

1. Durchsuchen von Backup-Jobs

Beim Durchsuchen von Backup-Jobs lädt Veeam Backup *for Microsoft 365* den letzten Wiederherstellungspunkt, der von dem ausgewählten Job erstellt wurde.

2. Durchsuchen einzelner Organisationen

Beim Durchsuchen einer einzelnen Organisation führt Veeam Backup *for Microsoft Office 365* die letzten Wiederherstellungspunkte, die von den einzelnen Backup-Jobs der ausgewählten Organisation erstellt wurden, zusammen und lädt sie.

3. Durchsuchen aller Organisationen

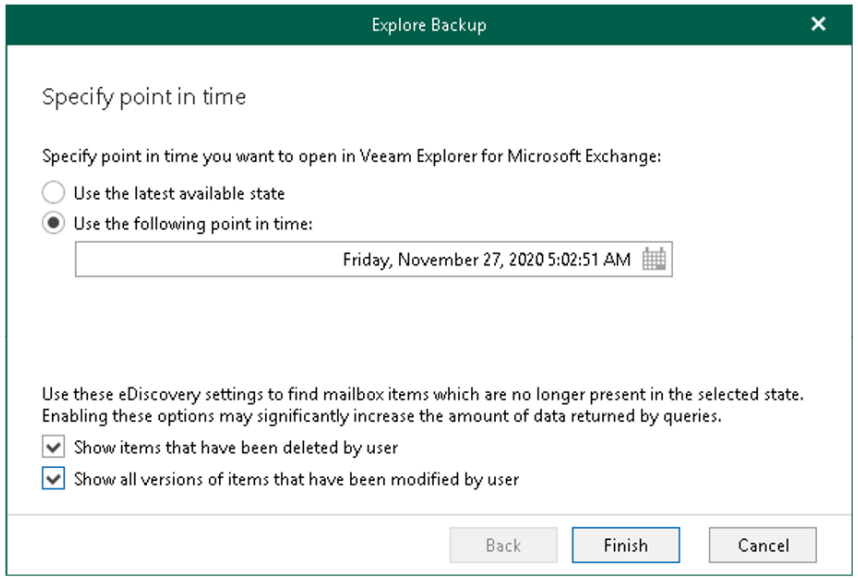
Beim Durchsuchen aller Organisationen führt Veeam Backup*for Microsoft 365* die letzten Wiederherstellungspunkte der einzelnen Backup-Jobs jeder Organisation zusammen und lädt sie.

4. Durchsuchen nach einem bestimmten Zeitpunkt

Beim Durchsuchen eines Status zu einem bestimmten Zeitpunkt wählen Sie einen Backup-Status, den Sie öffnen möchten.

Use the latest available state (Den letzten verfügbaren Status verwenden): Wählen Sie diese Option, um den letzten Status der Objekte in der Backup-Datei zu laden.

Use the following point in time (Den folgenden Zeitpunkt verwenden): Wählen Sie diese Option, um das Backup zu laden, das zum ausgewählten Zeitpunkt erstellt wurde.



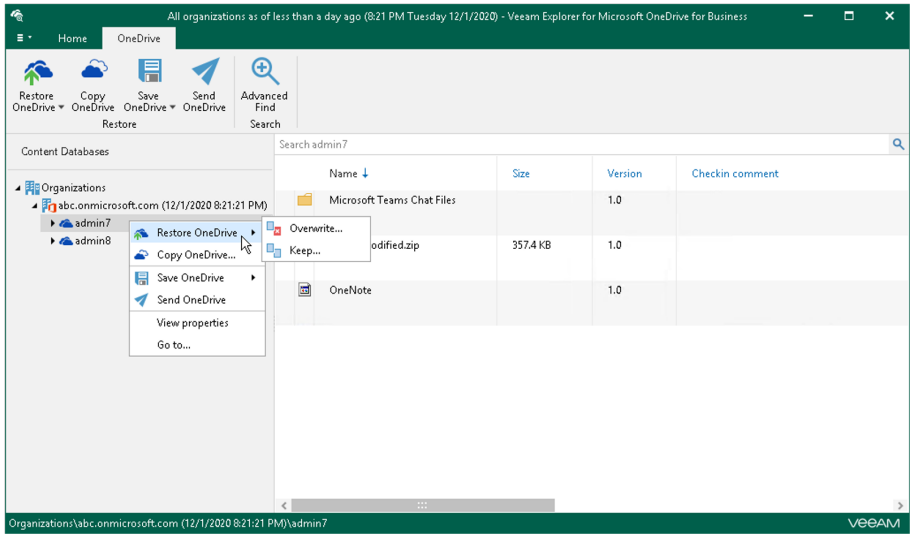
Wiederherstellung in drei Schritten: 1. Schritt

Die Wiederherstellung von Microsoft 365-Daten mit Veeam umfasst drei Schritte. Zunächst wird der Wiederherstellungsassistent aufgerufen. In diesem Beispiel wird gezeigt, wie Sie Daten aus OneDrive for Business wiederherstellen.

Starten Sie den Wiederherstellungsassistenten.

Öffnen Sie den **Wiederherstellungsassistenten** auf eine der folgenden Arten:

1. Wählen Sie ein Objekt aus, das Sie wiederherstellen möchten:
   - Zur Wiederherstellung eines OneDrive for Business-Kontos wählen Sie das entsprechende Konto in der Liste der Konten aus.
   - Zur Wiederherstellung eines Ordners wählen Sie den entsprechenden Ordner in der Liste der Ordner aus.
   - Zur Wiederherstellung eines Dokuments wählen Sie den Ordner mit dem gewünschten Dokument in der Liste der Ordner aus und wählen anschließend im Vorschaufenster das Dokument aus.
2. Klicken Sie auf dem Tab **OneDrive/Folder/Document** (OneDrive/Ordner/Dokument) auf **Restore OneDrive/Restore Folder/Restore Document** (OneDrive/Ordner/Dokument wiederherstellen) und wählen Sie eine der folgenden Optionen:
   - **Overwrite** (Überschreiben): Alle vorhandenen OneDrive-Daten werden überschrieben.
   - **Keep** (Beibehalten): Vorhandene Daten werden beibehalten und Objekte mit dem Präfix **RESTORED** (`RESTORED-<Dateiname>.ext`) wiederhergestellt.



Sie können auch mit der rechten Maustaste auf das wiederherzustellende Objekt klicken und **Restore OneDrive/Restore folder/Restore document > Overwrite** oder **Restore OneDrive/Restore folder/Restore document > Keep** (OneDrive/Ordner/Dokument wiederherstellen > Überschreiben bzw. Beibehalten) wählen.

Wiederherstellung in drei Schritten: 2. Schritt

Wählen Sie zwischen moderner oder einfacher Authentifizierung.

Moderne Authentifizierung

So verwenden Sie die moderne Authentifizierung:

1. Wählen Sie in der Dropdown-Liste **Specify the authentication method** (Authentifizierungsmethode festlegen) die Option **Modern authentication** (Moderne Authentifizierung).

Veeam Backup *for Microsoft 365* nutzt in diesem Fall eine Azure AD-Anwendung für die Wiederherstellung. Weitere Informationen finden Sie Im Kapitel Microsoft 365-Organisationen des Benutzerhandbuchs.

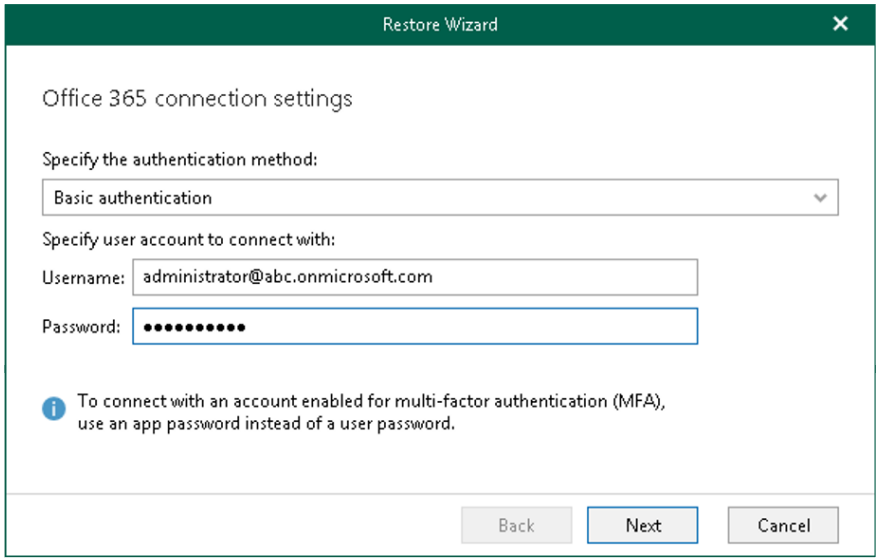
2. Geben Sie in das Feld **Application ID** (Anwendungs-ID) die ID der Azure AD-Anwendung ein, die für die Wiederherstellung genutzt werden soll. Veeam Explorer *for Microsoft OneDrive for Business* übernimmt in diesem Feld standardmäßig die ID der Anwendung, die in einer Backup-Session verwendet wurde. Wenn Sie eine andere Anwendung nutzen möchten, müssen Sie dieser die erforderlichen Berechtigungen erteilen. Weitere Informationen hierzu finden Sie im Kapitel Berechtigungen für die moderne, anwendungsbasierte Authentifzierung des Benutzerhandbuchs.

Einfache Authentifizierung

Die einfache Authentifizierung kann ausschließlich von Unternehmen genutzt werden, die noch Legacy-Authentifizierungsprotokolle unterstützen.
So verwenden Sie die einfache Authentifizierung:

1. Wählen Sie in der Dropdown-Liste **Specify the authentication method** (Authentifizierungsmethode festlegen) die Option **Basic authentication** (Einfache Authentifizierung).

2. Geben Sie die Anmeldedaten ein, um eine Verbindung zur SharePoint-Organisation herzustellen.



Wiederherstellung in drei Schritten: 3. Schritt

Dieser Schritt ist nur verfügbar, wenn Sie im vorherigen Schritt des Assistenten die Option **Modern authentication** gewählt haben.

In diesem Schritt melden Sie sich in Ihrer Microsoft 365-Organisation an.

So melden Sie sich in Ihrer Microsoft 365-Organisation an:

1. Klicken Sie auf **Copy code** (Code kopieren), um einen Authentifizierungscode zu kopieren.

Beachten Sie bitte, dass dieser Code nur 15 Minuten gültig ist. Durch Klicken auf **Refresh** (Aktualisieren) können Sie einen neuen Code von Microsoft anfordern.

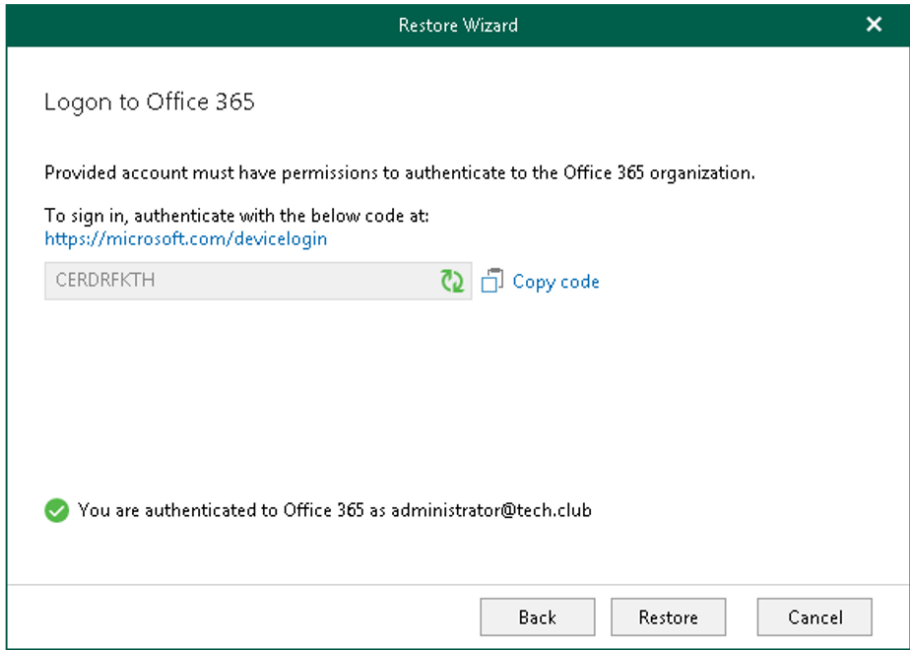
2. Klicken Sie auf den Link zum Portal von Microsoft.

3. Fügen Sie auf der Seite für die **Microsoft Azure-Geräteanmeldung** den kopierten Code ein und melden Sie sich in Azure an.

Verwenden Sie dabei ein Benutzerkonto mit den erforderlichen Berechtigungen. Für Veeam Explorer *for Microsoft OneDrive for Business* sind dieselben Berechtigungen erforderlich wie für Veeam Explorer *for Microsoft SharePoint*. Weitere Informationen finden Sie unter Erforderliche Berechtigungen.

Stellen Sie sicher, dass für die Azure AD-Anwendung, die für die Wiederherstellung genutzt werden soll, die richtigen Einstellungen konfiguriert sind. Weitere Informationen finden Sie im Kapitel Konfiguration von Azure AD-Anwendungseinstellungen des Benutzerhandbuchs.

4. Kehren Sie zum Wiederherstellungsassistenten zurück und klicken Sie auf „Restore" (Wiederherstellen).



Beachten Sie bitte, dass für die Wiederherstellung bestimmter Workloads zusätzliche Schritte erforderlich sind.

Self-Service-Portal für die Wiederherstellung

Veeam Backup *for Microsoft 365* kann eine Verbindung zum **Wiederherstellungsportal** herstellen. Über diese webbasierte Lösung können Nutzer ihre gesicherten Daten aus Microsoft Exchange, Microsoft SharePoint, Microsoft OneDrive for Business und Microsoft Teams durchsuchen und eigenständig wiederherstellen. Das Wiederherstellungsportal unterstützt zwei Szenarien für die Datenwiederherstellung: die **Self-Service-Wiederherstellung für Benutzer und die Self-Service-Wiederherstellung für Operatoren**. Wenn Sie *Benutzer* sind, stellen Sie Ihre Daten mittels Self-Service wieder her. Wenn Sie Operator-Berechtigungen haben, können Sie die gesicherten Daten für die Objekte, zu deren Management Sie berechtigt sind, durchsuchen und *wiederherstellen*.

Diese Komponenten kommen im Wiederherstellungsportal zum Einsatz:

- Veeam Backup *for Microsoft 365*-Server
- RESTful API-Service für Veeam Backup *for Microsoft 365*
- Microsoft 365-Organisation
- Wiederherstellungsportal
- Veeam Backup *for Microsoft 365*-Proxy-Service

Veeam Backup for Microsoft 365 nutzt RESTful APIs und Azure AD-Anwendungen, um Nutzer mit den Anmeldedaten für ihr Microsoft 365-Benutzerkonto im Wiederherstellungsportal zu authentifizieren. Die RESTful API-Autorisierung basiert auf dem OAuth 2.0 Authorization Framework.

Das Wiederherstellungsportal kommuniziert über eine RESTful API mit dem Veeam Backup *for Microsoft 365*-Server.

Der Datenaustausch zwischen dem Veeam Backup *for Microsoft 365*-Server, der Microsoft 365-Organisation, der Azure AD-Anwendung, dem RESTful API-Service für Veeam Backup *for Microsoft 365* und dem Wiederherstellungsportal basiert auf SSL-Zertifikaten.

Der Zugriff auf das Wiederherstellungsportal für Benutzer und Operatoren wird in sechs Schritten konfiguriert:

1. Vergewissern Sie sich, dass die RESTful API für Veeam Backup *for Microsoft 365* entweder auf dem Veeam Backup *for Microsoft 365*-Server oder auf einer separaten Maschine installiert ist.

Wenn Sie die RESTful API getrennt vom Veeam Backup *for Microsoft 365*-Server installieren, wird die Performance der Infrastruktur beim Durchsuchen und Wiederherstellen von Backup-Daten über das Wiederherstellungsportal weniger beeinträchtigt.

2. Aktivieren Sie den RESTful API-Service für Veeam Backup *for Microsoft 365*.

Dieser Service verarbeitet die RESTful API-Befehle und ermöglicht dem Wiederherstellungsportal die Kommunikation mit Veeam Backup *for Microsoft 365*.

3. Aktivieren Sie die Authentifizierung für Operatoren auf dem Veeam Backup *for Microsoft 365*-Server.

4. Aktivieren Sie das Wiederherstellungsportal und konfigurieren Sie den Zugriff.

5. Fügen Sie Operator-Rollen hinzu, um den entsprechenden Benutzern die erforderlichen Berechtigungen zu erteilen.

6. Informieren Sie Ihre Benutzer und Operatoren, über welche Internetadresse sie auf das Wiederherstellungsportal zugreifen können.

Self-Service-Portal für die Wiederherstellung

Über die unkomplizierte, intuitive Benutzeroberfläche des Wiederherstellungsportals können Benutzer ihre Daten eigenständig wiederherstellen. Operatoren können darüber die Wiederherstellung von Benutzern, Gruppen, Websites, Teams oder vollständigen Microsoft 365-Organisationen verwalten.

Das Hauptfenster im Überblick

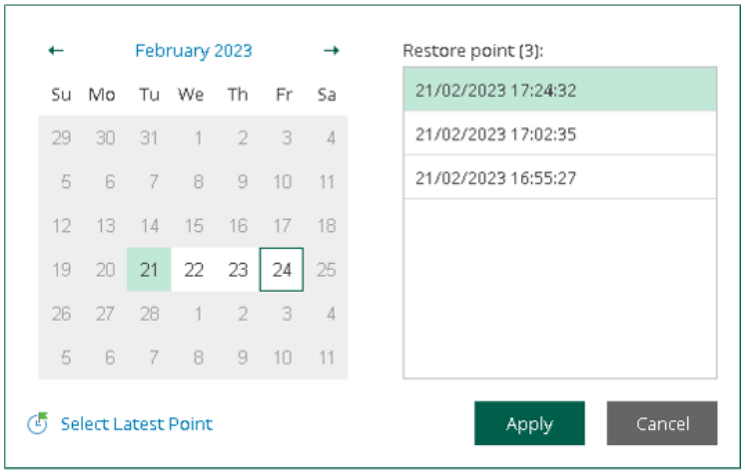
Das Hauptfenster beinhaltet die Tabs **Explore** (Durchsuchen), **Restore Sessions** (Wiederherstellungssessions) und **Restore List** (Wiederherstellungsliste).

- **Explore:** Dieser Tab enthält das Navigations- und Vorschaufenster.
  - Im Navigationsfenster können Sie das Objekt auswählen, das Sie (als Operator) verwalten möchten, oder einen Wiederherstellungspunkt festlegen.
  - Im Vorschaufenster können Sie Details zu den Objekten des Ordners anzeigen, den Sie im Navigationsfenster ausgewählt haben.
- **Restore Sessions:** Dieser Tab enthält Informationen zum Fortschritt und zu den Ergebnissen von Wiederherstellungssessions. Sie haben diese Möglichkeiten:
  - Anhalten einer Wiederherstellungssession.
  - Durchsuchen und Filtern von Wiederherstellungssessions nach Typ, Status und Zeitraum.
  - Anzeige der Liste von Ereignissen während einer Wiederherstellungssession sowie Durchsuchen und Filtern der Ereignisse nach ihrem Status.
- **Restore List:** Auf diesem Tab stehen Optionen für die Anzeige und Bearbeitung von Inhalten der Wiederherstellungsliste zur Verfügung. Dieser Tab wird nur angezeigt, wenn die Wiederherstellungsliste Objekte enthält. Sie haben diese Möglichkeiten:
  - Auswahl der wiederherzustellenden Objekte.
  - Löschen von Objekten aus der Wiederherstellungsliste.
  - Durchsuchen und Filtern von Objekten nach Wiederherstellungsstatus.
- Oben rechts im Hauptfenster wird ein *Benachrichtigungssymbol* in Form einer Glocke angezeigt, über das ein **Benachrichtigungsfenster** geöffnet werden kann.
  - Klicken Sie auf das Symbol, um das Benachrichtigungsfenster einzublenden.

Auswahl von Wiederherstellungspunkten in einem Backup

1. Klicken Sie oben links im Wiederherstellungsportal auf **Select Restore Point** (Wiederherstellungspunkt auswählen) oder auf den Zeitstempel des gewünschten Wiederherstellungspunkts.

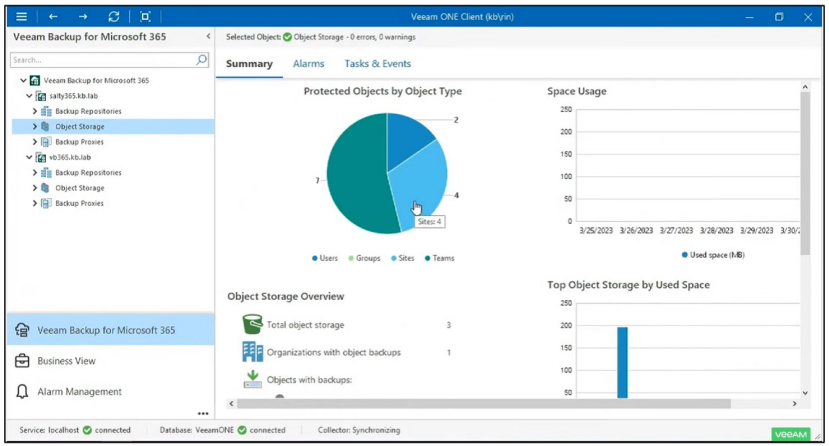
2. Führen Sie im angezeigten Dialogfenster einen dieser Schritte aus:
   - Klicken Sie im Kalender auf ein Datum, um die verfügbaren Wiederherstellungspunkte anzuzeigen. Sie sind in Fettschrift markiert. Die Liste verfügbarer Wiederherstellungspunkte für das gewählte Datum wird rechts angezeigt.
   - Klicken Sie auf **Select Latest Point** (Letzten Punkt auswählen), um den letzten im Backup-Repository verfügbaren Wiederherstellungspunkt auszuwählen.
   - Klicken Sie auf **Apply** (Übernehmen).

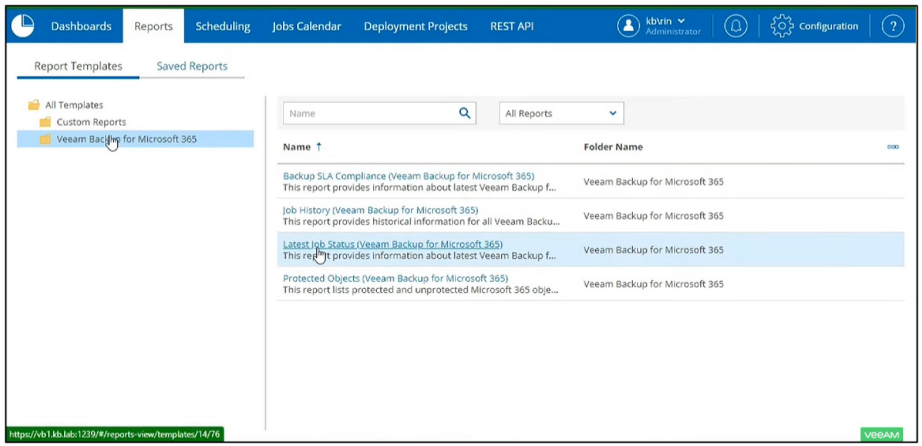


Erweitertes Monitoring und Reporting

Veeam Backup *for Microsoft 365* ermöglicht dank der Integration in **Veeam ONE v12** erweitertes Monitoring und Reporting. Für die Nutzung dieser Funktionalitäten ist eine separate Installation erforderlich, die für Kunden kostenlos ist. Die Software kann über die Download-Seite von Veeam Backup *for Microsoft 365* heruntergeladen werden. In dieser Demo wird die Installation erläutert.

- Nach der Installation können Sie über die Tabs verschiedene Aspekte Ihrer Backup-Infrastruktur überwachen.
- Auf dem Tab „Summary" (Überblick) werden die Objekte angezeigt, die gesichert werden, der Status von Backup-Jobs und die verfügbaren Kapazitäten Ihrer Storage-Repositorys. Über den Tab „Alarms" haben Sie Zugriff auf Benachrichtigungen zu potenziellen Backup-Problemen.
- Erweitern Sie die Anzeige der Objekte im Fenster links, um die einzelnen Jobs, Proxys und Repositorys anzuzeigen. Sie sehen dort auch, welche Objekte in den jeweiligen Repositorys gesichert werden.
- Unter „Alarm Management" (Benachrichtigungsverwaltung) werden vorkonfigurierte Benachrichtigungen angezeigt, die Sie mit verschiedenen Regeln anpassen können. Sie können unter anderem festlegen, welche Art von Benachrichtigungen Sie erhalten möchten, und Maßnahmen zur Fehlerbehebung definieren.
- Unter „Custom Reports" (Eigene Reports) können Sie Reports nach einem bestimmten Zeitplan oder nach Bedarf ausführen. Sie können Reports freigeben und eigene Dashboards für bestimmte Reporting- oder Compliance-Anforderungen erstellen.
- Es steht auch eine webbasierte Version dieser Lösung zur Verfügung, mit der Sie die wichtigsten Monitoring-Aktivitäten in einer täglichen Übersicht anzeigen können.





Worauf Sie achten sollten

- Wesentliche Unterscheidungsfaktoren
- Die Meinung unserer Kunden
- Fazit

Wesentliche Unterscheidungsfaktoren

Veeam Backup *for Microsoft 365* hat gegenüber anderen Lösungen einige entscheidende Vorteile. Die meisten Backup-Lösungen bieten nicht die notwendige Flexibilität oder Funktionalität, um die Datensicherung auf die individuellen Anforderungen eines Unternehmens abzustimmen.

Freie Wahl der Infrastruktur

Bleiben Sie Besitzer Ihrer Daten, indem Sie die Infrastruktur wählen, die Ihren geschäftlichen Anforderungen am besten entspricht, und diese bei Bedarf anpassen. Nahezu alle Cloud- und Hardwareplattformen werden unterstützt.

SaaS-Anbieter bieten in der Regel nur eingeschränkte Unterstützung für unterschiedliche Clouds und zwingen Kunden unter Umständen sogar zur Nutzung ihrer Cloud. Nach der Konfiguration sind Änderungen nur selten möglich.

Kontrolle der Datensicherung

Behalten Sie die Kontrolle, indem Sie den einzelnen Nutzern die Datensicherungsfunktionen bereitstellen, die dem geschäftlichen Wert ihrer jeweiligen Daten entsprechen.

SaaS-Anbieter ermöglichen nur selten eine Anpassung der Backup-Häufigkeit, sodass Unternehmen ihre Datensicherung nicht auf die Anforderungen ihrer Anwender abstimmen können.

Flexible Wiederherstellung

Minimieren Sie Ausfallzeiten, indem Sie Daten sinnvoll wiederherstellen – unabhängig von der Art des Datenverlusts.

Bei manchen Lösungen lassen sich Ausfallzeiten nach einem Datenverlust nur eingeschränkt minimieren, da Daten möglicherweise nicht den Anforderungen eines Unternehmens entsprechend wiederhergestellt werden können.

Die Meinung unserer Kunden

Die meisten Kunden, die Veeam Backup *for Microsoft 365* einsetzen, sind begeistert. Auf Bewertungsplattformen wie TrustRadius und G2 Crowd können Sie sich davon überzeugen und ungefilterte Meinungen zum Produkt lesen.

Nutzen Sie Veeam Backup *for Microsoft 365* – Ihr Chef wird begeistert sein!

„Cloud-Services haben ihre Nachteile, weshalb es letztlich in der Verantwortung des Systemadministrator liegt, für Datensicherheit zu sorgen. Veeam Backup *for Microsoft 365* hält sein Versprechen und gibt dem Administrator die Kontrolle über die Daten."

– IT-Administrator
Personalagentur
1.001 - 5.000 Mitarbeiter

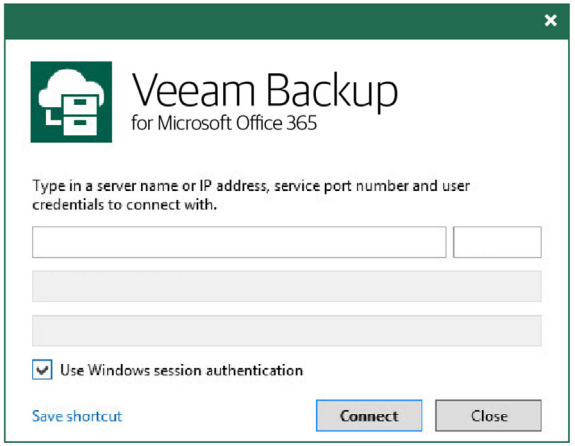
Mit Veeam *Backup for Microsoft Office 365* lassen sich Daten individuell sichern!

„Wir können damit ein großes Problem mit Microsoft 365 lösen, nämlich die fehlende Kontrolle über unsere Daten. Bei Microsoft 365 weiß man oft nicht, wo die Daten gespeichert sind und wie man sie im Notfall wiederherstellen kann. Mit Veeam Backup *for Microsoft 365* können wir sicherstellen, dass unsere Daten zuverlässig geschützt sind."

– Systemadministrator
Moses Lake Industries
Halbleiterhersteller |
201 - 500 Mitarbeiter

Überzeugen Sie sich

Testversion herunterladen
KOSTENLOS für 30 Tage

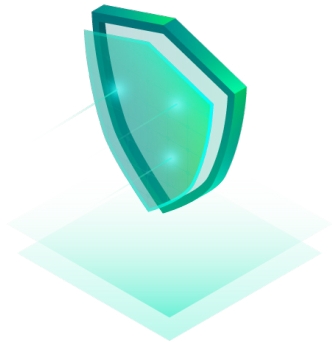


Fazit

Bei Microsoft 365 haben Sie die Kontrolle über Ihre Daten – sind aber auch für deren Schutz verantwortlich.

Veeam Backup *for Microsoft 365* minimiert das Risiko, nicht mehr auf Microsoft 365-Daten in Exchange Online, SharePoint Online, OneDrive for Business und Microsoft Teams zugreifen zu können. Sie profitieren damit von umfassender Kontrolle, zuverlässigem Schutz und unterbrechungsfreier Verfügbarkeit Ihrer Daten.

Mit Veeam können Sie Microsoft 365-Daten auf beliebigen Zielsystemen speichern: in Ihrer lokalen Umgebung, in Azure, in AWS oder bei einem Serviceprovider. Weitere Vorteile:



Schutz Ihrer Microsoft 365-Daten vor versehentlicher Löschung, Sicherheitsbedrohungen und Lücken in Aufbewahrungsrichtlinien

Schnelle Wiederherstellung einzelner Microsoft 365-Objekte und -Dateien mit branchenführenden, flexiblen Optionen

Einhaltung gesetzlicher Bestimmungen und Compliance-Vorgaben mit effizientem e-Discovery von Microsoft 365-Backup-Archiven

Testversion herunterladen
KOSTENLOS für 30 Tage