MICROSOFT 365 · BACKUP · SHAREPOINT, ONEDRIVE, EXCHANGE

Microsoft 365 Backup: Full Workload Backup für SharePoint, OneDrive und Exchange geht in GA

Consulting Briefing · 23. September 2026 · boddenberg.de · Lesezeit rund 10 Minuten

Executive Summary

Microsoft 365 Backup kann ab sofort, was man eigentlich vom ersten Tag an erwartet hätte: einen kompletten Workload mit einer einzigen Policy sichern. Ein Haken bei „Alle SharePoint-Sites“, einer bei „Alle OneDrive-Konten“, einer bei „Alle Postfächer“ – fertig. Der GA-Rollout läuft laut Message Center MC1387526 seit Mitte September und soll bis Mitte Oktober 2026 abgeschlossen sein. Die Public Preview lief seit Anfang Juli.

Warum das mehr ist als ein Komfort-Feature? Bisher musstest du jede Site, jedes OneDrive und jedes Postfach einer Policy zuordnen – per CSV, per Filter oder per Hand. Das klappt am Tag der Einführung wunderbar. Acht Monate später hat das Marketing 40 neue Teams angelegt, die Fusion hat 300 Postfächer mitgebracht, und niemand hat die Policy angefasst. Im Ernstfall stellst du dann fest, dass genau die Site, die der Verschlüsselungstrojaner gefressen hat, nie gesichert wurde. Full Workload Backup schließt diese Lücke: Neue Objekte werden alle 24 Stunden erkannt und automatisch geschützt.

Die Kehrseite steht auf der Rechnung. Microsoft 365 Backup kostet 0,15 US-Dollar pro Gigabyte geschützter Daten und Monat, Wiederherstellungen sind kostenlos. „Alles sichern“ heißt also auch „alles bezahlen“ – inklusive der Testsite von 2019, die niemand mehr kennt, aber jeder behalten will. Deine Aufgabe ist deshalb nicht, einen Schalter umzulegen, sondern vorher zu entscheiden, was nicht gesichert werden soll.

FAKTEN · Das Wichtigste in fünf Zeilen

Eine Policy pro Workload, separat aktivierbar für SharePoint, OneDrive und Exchange. Custom-Policies haben immer Vorrang. Ausschlüsse per CSV, bis zu 10.000 Objekte pro Vorgang. Neue Sites, Konten und Postfächer werden alle 24 Stunden aufgenommen. Das Feature ist standardmäßig verfügbar, muss aber aktiv eingeschaltet werden – von allein passiert nichts.

Worum geht es im Detail?

Hintergrund: Warum Microsoft überhaupt Backup verkauft

Lange war die Microsoft-Antwort auf die Backup-Frage ein freundliches Achselzucken: Papierkorb, Versionierung, Aufbewahrungsrichtlinien, georedundante Rechenzentren – wozu noch ein Backup? Die Antwort liefert jeder, der einmal eine Ransomware-Attacke auf einen OneDrive-Client

erlebt hat. Der Sync-Client verschlüsselt fröhlich mit, die Versionen stapeln sich, und das Zurückrollen von 80.000 Dateien per Hand ist eine Beschäftigungstherapie, die kein Mensch überlebt. Redundanz schützt vor dem abgebrannten Rechenzentrum, nicht vor dem eigenen Admin mit schlechtem Tag.

Microsoft 365 Backup setzt genau da an. Der Clou: Die Sicherungen liegen innerhalb der Microsoft-365-Vertrauensgrenze, auf derselben Infrastruktur wie SharePoint und Exchange, in append-only Speicher. Alte Sicherungen lassen sich also nicht überschreiben, nur neue hinzufügen. Weil die Daten beim Restore das Rechenzentrum nicht verlassen, ist die Wiederherstellung schnell: Eine Site unter einem Terabyte ist mit einem Express-Restore-Punkt in unter 20 Minuten zurück, bei Massenwiederherstellungen spricht Microsoft von bis zu 250 Objekten pro Stunde und bis zu 2 TB pro Stunde im Median.

Was Full Workload Backup konkret macht

Im Admin Center wählst du unter Einstellungen → Microsoft 365 Backup für einen Workload „Alle Sites“ beziehungsweise „Alle OneDrive-Konten“ oder „Alle Postfächer“. Ein Bestätigungsdialog weist dich auf mögliche Kostenfolgen hin – der einzige Moment, in dem Microsoft dich vor dir selbst schützt. Danach kannst du optional eine CSV mit Ausschlüssen hochladen, und das System legt eine Policy wie „Full SharePoint Backup“ an.

Entscheidend ist die Rangfolge. Ein Objekt, das schon in einer Custom-Policy steckt – egal ob aktiv oder pausiert –, fasst die Full-Workload-Policy nicht an. Nimmst du ein Objekt, das bisher über Full Workload geschützt war, in eine Custom-Policy auf, zieht es ohne Lücke in den Restore-Punkten um. Entfernst du es dagegen aus der Full-Workload-Policy, landet es automatisch auf der Ausschlussliste, damit es beim nächsten 24-Stunden-Scan nicht sofort wieder eingesammelt wird. Schaltest du das Feature ganz ab, verschwindet die Policy, die betroffenen Objekte wandern in „Entfernte Elemente“, und ihre alten Sicherungen bleiben bis zum Ende des Recovery-Fensters erhalten.

Merkmal	Custom-Policy	Full-Workload-Policy
Umfang	Handverlesen: CSV, Filter, dynamische Gruppenregeln oder Einzelauswahl	Alles Berechtigte im Workload, abzüglich Ausschlüsse
Neue Objekte	Nur über dynamische Regeln (Preview) oder manuell	Automatisch, Scan alle 24 Stunden
Anzahl	Bis zu 100 Policies pro Workload, je 100.000 Objekte	Genau eine pro Workload
Vorrang	Gewinnt immer	Greift nur, wo keine Custom-Policy greift
Typischer Einsatz	Abweichende Recovery-Fenster, Kostenstellen, Sonderfälle	Grundschutz für den ganzen Rest

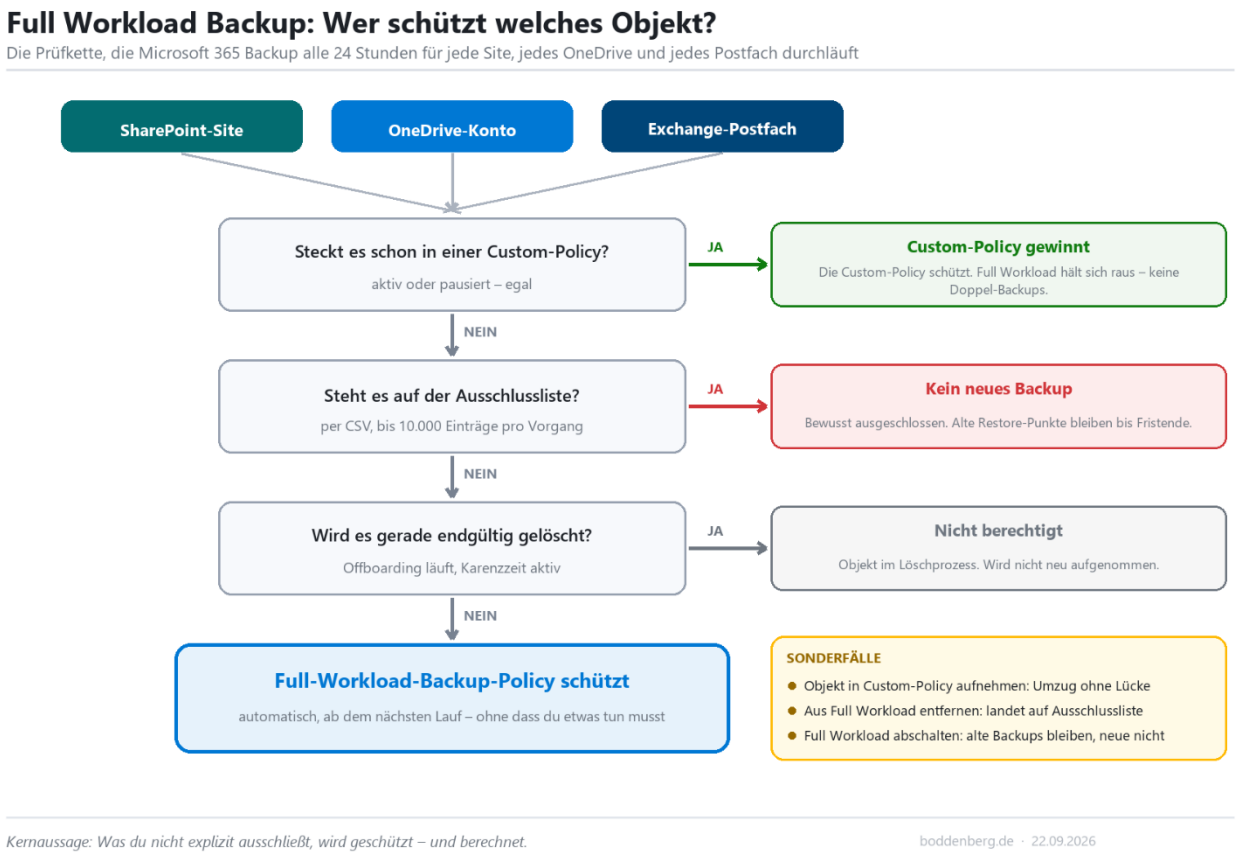

Abbildung 1: Die Prüfkette hinter Full Workload Backup – Custom-Policy schlägt Ausschlussliste schlägt Automatik.

Restore-Punkte, Recovery-Fenster und Grenzen

Für SharePoint und OneDrive gibt es zwei Wochen lang alle zehn Minuten einen Restore-Punkt, danach wöchentliche Snapshots. Exchange bekommt Zehn-Minuten-Punkte über das ganze Jahr. Das Recovery-Fenster stellst du pro Policy auf drei, sechs, zwölf oder 24 Monate; Standard ist ein Jahr. Verkürzt du es, greift eine Karenzzeit von 30 Tagen, bevor alte Punkte gelöscht werden – ein eingebauter Schutz gegen den Admin, der „mal eben Kosten spart“, und gegen den Angreifer, der genau das vortäuscht.

Die Obergrenzen sind großzügig, aber nicht unendlich: bis zu einer Million Objekte pro Workload. Wer mehr hat, muss mit Microsoft reden. Und nicht alles ist sicherbar: In Exchange werden Benutzer- und freigegebene Postfächer unterstützt, Raum- und Gruppenpostfächer derzeit nicht. Einige alte SharePoint-Site-Vorlagen fallen ebenfalls raus. Teams-Dateien liegen in SharePoint und sind damit drin; Entra-Objekte, Planner oder Power-Platform-Inhalte deckt Microsoft 365 Backup dagegen gar nicht ab.

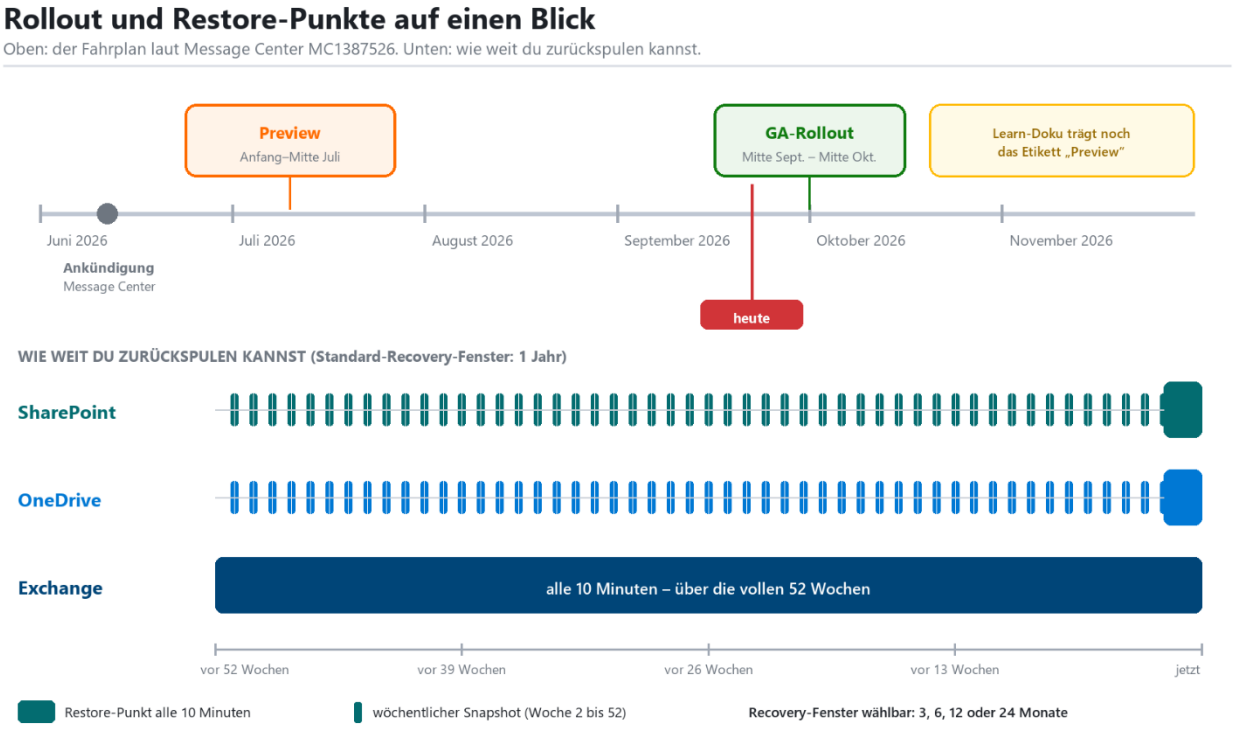

Abbildung 2: Rollout-Fahrplan laut MC1387526 und die Dichte der Restore-Punkte je Workload.

Was sind Chancen? Was sind Risiken?

Die größte Chance ist langweilig, und genau deshalb wertvoll: Du musst dich nicht mehr daran erinnern, neue Objekte in die Sicherung aufzunehmen. Backup-Lücken entstehen fast nie durch technisches Versagen, sondern durch Vergessen. Ein Kunde von uns hat beim ersten Restore-Test festgestellt, dass sein Vertriebs-Team seit einer Reorganisation auf neuen Sites arbeitete – ungesichert, seit elf Monaten. Der Test war der Glücksfall; der Ernstfall wäre ein Karriereende gewesen.

Zweite Chance: Governance-Fälle werden schneller. Ein Abteilungsleiter löscht im Frust vor seinem Abgang den halben Projektordner? Ein Praktikant räumt die Site „Archiv_alt_final2“ auf, die sich als Vertragsablage entpuppt? Mit flächendeckender Sicherung ist das kein Ticket mit offenem Ausgang mehr, sondern ein Restore auf einen Zeitpunkt vor dem Drama – wahlweise an dieselbe oder eine neue URL, damit du erst prüfen kannst, bevor du überschreibst.

Die Risiken, über die im Vertriebsgespräch keiner redet

Risiko Nummer eins ist die Rechnung. Das Modell ist Pay-as-you-go über ein Azure-Abonnement, abgerechnet nach geschützter Datenmenge. Wer Full Workload für alles einschaltet, sichert auch die 4 TB Videoaufzeichnungen, die das Schulungsteam „nur vorübergehend“ in einer Site parkt. Und: Entfernst du Objekte aus einer Policy, kosten ihre vorhandenen Sicherungen weiter, bis das Recovery-Fenster abläuft. Das Backup vergisst nichts – der Controller auch nicht.

Chance	Risiko
Keine vergessenen Sites, Konten oder Postfächer mehr	Kosten wachsen automatisch mit jeder neuen Site mit
Schnelle Wiederherstellung innerhalb der Microsoft-Cloud	Sicherung liegt im selben Anbieter-Ökosystem – kein echter Medienbruch
Append-only-Speicher, 90 Tage Karenz nach Offboarding	Globale Admins mit bösen Absichten können das Offboarding trotzdem anstoßen
Weniger Policy-Pflege, klare Vorrangregeln	Unklare Zuständigkeit: Wer entscheidet über Ausschlüsse?
Purview-Löschrichtlinien lassen das Backup unberührt	Datenschutz: Gelöschtes lebt im Backup bis zum Fristende weiter

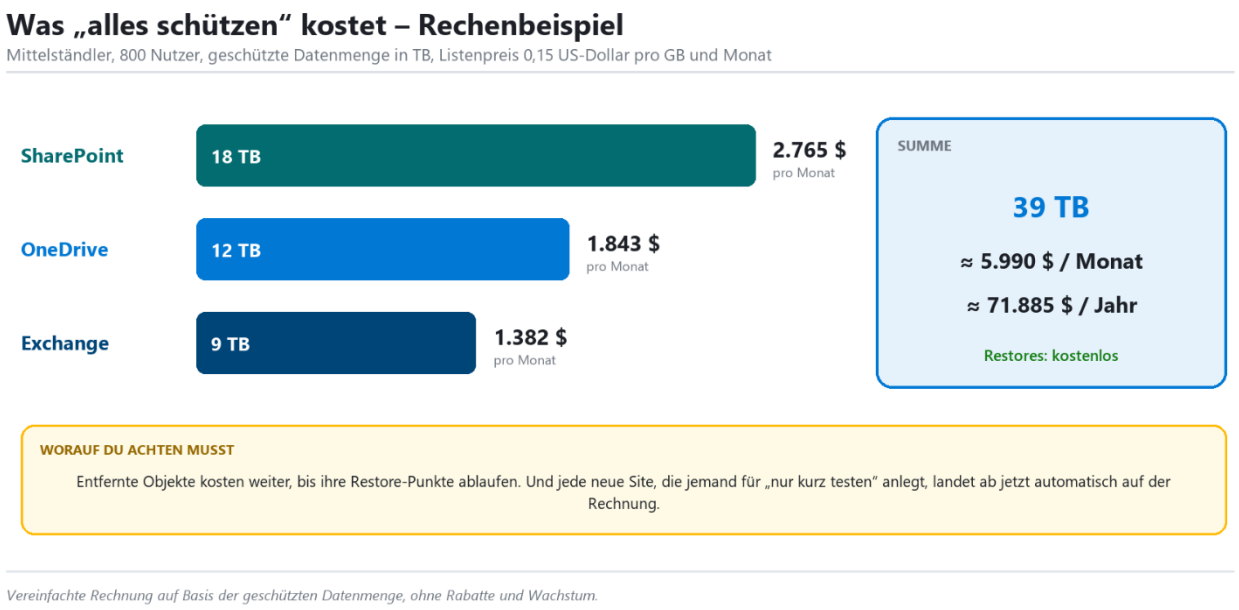

Abbildung 3: Beispielrechnung für einen Tenant mit 800 Nutzern und 39 TB geschützten Daten.

Risiko Nummer zwei ist architektonisch. Microsoft 365 Backup lebt im selben Tenant, auf derselben Plattform, unter denselben Admin-Konten wie die Produktivdaten. Microsoft baut Schutzmechanismen ein: append-only Speicher, 90 Tage Karenz nach dem Offboarding, Benachrichtigung mehrerer Admins bei riskanten Aktionen. Aber die klassische 3-2-1-Regel – drei Kopien, zwei Medien, eine außer Haus – erfüllst du damit allein nicht. Für viele Mittelständler ist das akzeptabel. Für Banken, Versicherer und alle, die unter DORA oder NIS2 eine unabhängige Kopie nachweisen müssen, eher nicht.

WARNUNG · Das Backup ist so sicher wie dein Global Admin

Wenn ein Angreifer ein Konto mit Global-Admin-Rechten übernimmt, hat er Zugriff auf Produktivdaten und Backup-Konsole gleichzeitig. Die 90-Tage-Karenz rettet dich nur, wenn du in diesen 90 Tagen merkst, dass jemand dein Backup offboardet hat. Privileged Identity Management, phishingresistente MFA und ein Alarm auf Backup-Aktionen sind Pflicht, keine Kür.

Risiko Nummer drei ist datenschutzrechtlich. Purview-Aufbewahrungs- und Löschrichtlinien beeinflussen das Backup ausdrücklich nicht. Das ist technisch gewollt, damit niemand die Sicherung über eine Löschrichtlinie aushebeln kann. Für deinen Datenschutzbeauftragten heißt es aber: Ein gelöschtes Postfach eines ehemaligen Mitarbeiters existiert im Backup weiter, bis das Recovery-Fenster endet. Das gehört ins Verarbeitungsverzeichnis und in die Löschkonzept-Doku, bevor die erste Auskunftsanfrage kommt.

Was müssen wir jetzt schon vorbereiten?

Gute Nachricht: Vor dem Rollout ist keine Aktion zwingend. Schlechte Nachricht: Wer einfach nur den Schalter umlegt, hat in drei Monaten eine Diskussion mit dem Controlling. Die Vorbereitung ist zu 80 Prozent Organisation und zu 20 Prozent Klicken.

Schritt	Was genau	Wer	Bis wann
1. Bestand aufnehmen	Speicherbericht aus dem Admin Center: Datenmenge je Workload, größte Sites und Postfächer	M365-Admin	Oktober
2. Kosten schätzen	Datenmenge × 0,15 US-Dollar, plus Wachstum; Budget im Azure-Abo reservieren	IT-Leitung, Controlling	Oktober
3. Ausschlüsse festlegen	Archive, Test-Sites, Video-Ablagen, Datenfriedhöfe; CSV vorbereiten	Fachbereiche, Datenschutz	vor Aktivierung
4. Sonderfälle abbilden	Custom-Policies für abweichende Recovery-Fenster, z. B. Geschäftsleitung 2 Jahre	M365-Admin	vor Aktivierung
5. Admin-Konten härten	PIM, phishingresistente MFA, Alarm auf Backup-Änderungen	Security	sofort
6. Restore üben	Eine Site an neue URL, ein Postfach-Ordner, Zeit messen, dokumentieren	M365-Admin	nach Aktivierung

TIPP · Erst Custom, dann Full Workload

Lege deine Sonderfälle – Geschäftsleitung, Rechtsabteilung, kritische Projekte – zuerst als Custom-Policies mit passendem Recovery-Fenster an. Danach schaltest du Full Workload als Grundschutz für den Rest ein. Umgekehrt geht es auch, dank lückenlosem Umzug, aber so herum behältst du den Überblick.

Ein Wort zu Multi-Geo: Satellitenstandorte lassen sich in Custom-Policies nur über den CSV-Upload aufnehmen, die Oberfläche kennt nur den zentralen Standort. Prüfe nach der Aktivierung, ob Full Workload deine Satelliten wirklich mitnimmt, bevor du dich darauf verlässt. Die Daten bleiben übrigens in der jeweiligen Geo, die Residency-Vorgaben werden eingehalten.

WICHTIG · Ein Backup, das nie getestet wurde, ist eine Vermutung

Plane den ersten Restore-Test direkt nach der Aktivierung ein – nicht „wenn mal Zeit ist“. Stell eine echte Site an eine neue URL wieder her und miss die Zeit. Zwischen „dauert 20 Minuten“ im Datenblatt und „dauert 20 Minuten“ in deinem Tenant liegen oft eine vergessene Berechtigung und ein verärgerter Fachbereich.

Und schließlich: Überlege, ob Microsoft 365 Backup dein einziges Backup sein soll. Partner wie die großen Backup-Hersteller setzen auf derselben Microsoft 365 Backup Storage-Plattform auf und liefern zusätzlich eine zentrale Konsole für den restlichen Datenbestand. Für echte Unabhängigkeit brauchst du trotzdem eine Kopie außerhalb des Tenants. Die Frage ist nicht, ob du paranoid bist, sondern ob du es dir leisten kannst, es nicht zu sein.

Häufig gestellte Fragen

Was kostet Microsoft 365 Backup?

Microsoft 365 Backup wird nach Verbrauch über ein Azure-Abonnement abgerechnet und kostet 0,15 US-Dollar pro Gigabyte geschützter Daten und Monat. Wiederherstellungen sind kostenlos, zusätzliche Benutzerlizenzen sind nicht nötig.

Werden neue SharePoint-Sites mit Full Workload Backup automatisch gesichert?

Ja, Microsoft 365 Backup prüft alle 24 Stunden auf neue SharePoint-Sites, OneDrive-Konten und Exchange-Postfächer und nimmt sie automatisch in die Full-Workload-Policy auf. Ausgenommen sind nur Objekte auf der Ausschlussliste oder in einer Custom-Policy.

Kann ich einzelne Sites oder Postfächer vom Full Workload Backup ausschließen?

Ja, über eine Ausschlussliste, die du per CSV-Datei pflegst; pro Vorgang lassen sich bis zu 10.000 Objekte ausschließen. Ausgeschlossene Objekte kannst du trotzdem jederzeit über eine eigene Custom-Policy sichern.

Wie lange bewahrt Microsoft 365 Backup Sicherungen auf?

Das Recovery-Fenster ist pro Policy auf drei, sechs, zwölf oder 24 Monate einstellbar, Standard ist ein Jahr. Eine Verkürzung wird erst nach einer Karenzzeit von 30 Tagen wirksam, damit versehentliche oder böswillige Änderungen auffallen.

Ersetzt Microsoft 365 Backup eine Drittanbieter-Backup-Lösung?

Für schnelle Wiederherstellung von SharePoint, OneDrive und Exchange ist es sehr stark, deckt aber weder Entra ID noch Planner oder Power Platform ab und liegt im selben Tenant wie die Produktivdaten. Wer eine unabhängige Kopie nach der 3-2-1-Regel braucht, benötigt zusätzlich eine Sicherung außerhalb von Microsoft 365.