



NAKIVO Backup und Ransomware-Schutz für Microsoft 365



Microsoft Teams

Exchange
OnlineOneDrive
for Business

SharePoint

VORTEILE

2X

schneller mit inkrementellen Backups

49%

geringere Kosten im Vergleich zu anderen Anbietern

4.8 STERNE

durchschnittliche Bewertung für Zeit- und Geldersparnis

15 SPEICHERORTE

für erhöhte Redundanz und Sicherheit

4.000

Wiederherstellungspunkte pro Backup-Job für eine flexiblere und präzisere Wiederherstellung

5 MINUTEN

für die Bereitstellung und Einrichtung der Lösung

MICROSOFT 365 IST NICHT VOR DATENVERLUST GESCHÜTZT

Obwohl Microsoft für die Sicherheit und Verfügbarkeit seiner Infrastruktur verantwortlich ist, liegt die Sicherung von Kundendaten in Microsoft 365 allein in der Verantwortung des Kunden. Um den Verlust kritischer Daten zu vermeiden und die Einhaltung gesetzlicher Vorschriften sicherzustellen, benötigen Sie eine dedizierte Backup- und Wiederherstellungslösung für Microsoft 365.

NAKIVO Backup & Replication bietet ein All-in-One-Backup, sofortige granulare Wiederherstellung und Ransomware-Schutz für Microsoft Teams, Exchange Online, OneDrive for Business und SharePoint Online.

Mit robuster Datensicherung, sicherer Archivierung und optimierten Compliance-Funktionen hilft Ihnen die Lösung, den reibungslosen Betrieb und die Verfügbarkeit von Daten in jeder Situation aufrechtzuerhalten.

WICHTIGE GRÜNDE FÜR DIE SICHERUNG IHRER MICROSOFT 365-DATEN

Menschliches Versagen

Menschliches Versagen, wie z. B. versehentliches Löschen, ist die Hauptursache für Datenverlust. Solche Fehler können irreversiblen Schaden verursachen, der durch Microsoft 365-Backups leicht verhindert werden kann.

Cybersecurity-Bedrohungen

Fortschrittliche Ransomware, die auf Cloud-Daten abzielt, nimmt zu. Auch Insider-Bedrohungen stellen ein erhebliches Risiko für Ihre Daten dar.

Komplizierte Aufbewahrungsrichtlinien

Die nativen Aufbewahrungsrichtlinien von Microsoft 365 ersetzen keine Backups und werden oft missverstanden oder falsch genutzt.

Regulatorische Risiken

Unternehmen können mit ernsthaften rechtlichen Sanktionen belegt werden, wenn sie Daten nicht rechtzeitig an Aufsichts- oder Justizbehörden übermitteln.

Komplexe Datenarchitektur

Die vielfältigen und dynamischen Daten in Microsoft 365, die über verschiedene Apps verknüpft sind, machen manuelle Backups fehleranfällig, zeitaufwendig und teuer.

ERREICHEN SIE IHRE BACKUP- UND WIEDERHERSTELLUNGSZIELE

“ Wir sichern seit über 2 Jahren **2.500 Microsoft 365-Benutzerkonten**. Wir schätzen die Enterprise-Funktionen, die es uns ermöglichen, Microsoft 365 und unsere VMware-Umgebung vor Ort über eine einzige Benutzeroberfläche zu schützen und wiederherzustellen.

Robin Damen,
CEO bei Virtual Computing

“ Wir haben uns für NAKIVO für Microsoft 365 entschieden, um unsere **110 Postfächer zu sichern**. Der größte Vorteil ist die Möglichkeit, ganze Postfächer, ausgewählte Dateien und Ordner im Falle einer Löschung wiederherzustellen.

Lars Weimar, Leiter der
IT-Abteilung bei HAM Precision

“ Wir **zahlen einen minimalen Betrag pro Nutzer für ein Jahr** und sind sehr zufrieden, dass alle Microsoft 365-Anwendungen geschützt sind. Bei Bedarf ist der technische Support schnell erreichbar und steht über einen Online-Chat zur Verfügung.

Omer Akosman, IT-Manager im
Ottoman's Life Hotel Deluxe

NUTZEN SIE DAS VOLLE POTENZIAL IHRER MICROSOFT 365-BACKUPS

Vollständiger Schutz

Erstellen Sie vollständige und inkrementelle Backups von Exchange Online, SharePoint Online, OneDrive for Business und Microsoft Teams – alles zentral verwaltet über eine einzige Benutzeroberfläche.

Vielfältige Speicherziele

Speichern Sie Backups flexibel in lokalen Verzeichnissen, SMB/NFS-Shares, öffentlichen Cloud-Speicherplattformen, S3-kompatiblen Speicherzielen oder auf Deduplizierungsgeräten.

Direktes Backup in der Cloud

Senden Sie Microsoft 365-Backups direkt an Amazon S3, Wasabi, Azure Blob, Backblaze B2 und andere S3-kompatible Object-Storage-Ziele.

Backupkopie

Automatisieren Sie die Erstellung und Übertragung von Backup-Kopien zu externen Standorten wie Bandmedien, Cloud-Plattformen oder anderen S3-kompatiblen Speicherlösungen.

Vor Ransomware geschützte Backups

Schützen Sie Ihre Daten vor Ransomware mit unveränderbaren Backups in lokalen, Cloud- und S3-kompatiblen Speicherorten sowie abgeschotteten Kopien auf Band.

Sofortige granulare Wiederherstellung

Stellen Sie Microsoft 365-Daten in Sekunden wieder her – ob E-Mails, Anhänge, Ordner, Dateien, In-Place-Archive-Mailboxes, Litigation Hold-Elemente, Websites oder Kanäle – in das ursprüngliche oder ein anderes Konto.

Gartner®

Peer Insights™

Anerkannt im 2024 **Gartner® Peer Insights™**

Voice of the Customer

de soluciones empresariales de backup
y recuperación en 2024

**WERDEN SIE TEIL
VON 29 000+ KUNDEN
WELTWEIT**



Gartner® Magic Quadrant™ 2022

Lobende Erwähnung in
der Kategorie Backup- und
Wiederherstellungslösungen
für Unternehmen

**SIND SIE BEREIT,
LOSZULEGEN?**

GRATIS TESTEN

KOSTENLOSE DEMO ERHALTEN

MICROSOFT 365-DATENSCHUTZ – OPTIMIERT FÜR IHRE ANFORDERUNGEN

Sicherstellung der Betriebskontinuität

Mit Backups, die an mehreren Speicherorten verfügbar sind, stellen Sie Ihre Daten nach Störungen schnell wieder her und sichern eine maximale Betriebszeit sowie durchgehende Produktivität.

Volle Kontrolle behalten

Lokale Backup-Speicherung ermöglicht nicht nur eine schnelle Wiederherstellung, sondern erhöht auch die Sicherheit und gewährleistet die vollständige Kontrolle über Ihre Daten.

Einfache Datenversionierung

Mit flexiblen Aufbewahrungs- und Rotationsoptionen können Sie punktgenaue Wiederherstellungen der gewünschten Datenversion durchführen.

Effiziente Archivierung und Compliance

Ein strukturiertes Backup-Framework mit langfristiger Aufbewahrung, sofortiger Wiederherstellung und leistungsstarken Suchfunktionen unterstützt Sie dabei, Archivierungsvorgaben zu erfüllen und E-Discovery-Anfragen effizient zu bearbeiten.

Maximale Backup-Sicherheit

Durch starke Verschlüsselung, Multi-Faktor-Authentifizierung und rollenbasierte Zugriffskontrollen schützen Sie Microsoft 365-Backups umfassend vor unbefugtem Zugriff und Cyberbedrohungen.

