Solution Profile

2025-26 DCIG TOP 5

MICROSOFT 365 SAAS BACKUP SOLUTIONS // MIDMARKET EDITION

Spanning Backup for Microsoft 365

By

Jerome M Wendt, Principal Analyst
Ken Clipperton, Principal Researcher
Todd Dorsey, Sr. Storage Analyst
Joshua Konkle, Consulting Researcher

Table of Contents

Microsoft 365 SaaS Backup Solutions // Midmarket Edition

Spanning Backup for Microsoft 365

2025 DCIG 2026
TOP 5
M365 SaaS
BACKUP
MIDMARKET EDITION

SOLUTION

Spanning Backup for Microsoft 365

COMPANY

Kaseya
701 Brickell Ave #400
Miami, FL 33131
(833) 217-4284
spanning.com

DISTINGUISHING FEATURES OF SPANNING BACKUP FOR MICROSOFT 365

- 99.9% reliable restore SLA guarantee.
- Dark Web Monitoring monitors and scans dark web for data breach records.
- Immutable, tamper-proof audit logs of all backup and restore activities.
- Offers SaaS backup for Google Workspace and Salesforce.
- Regional data centers to meet data sovereignty requirements.
- Uses AWS' services to automate and simplify ongoing Backup for Microsoft 365's ongoing management.

CATEGORIES OF FEATURES EVALUATED

- Backup.
- Billing, configuration, & licensing.
- Cyber resilience.
- Recovery and restore.
- Technical support and service.

Organizations Deepen and Expand Their Use of Microsoft 365

2025 officially represents the twelfth year in which organizations have had access to Microsoft 365 *(formerly known as Office 365).*[1] From its humble beginnings in 2013, its stratospheric growth began in 2020 during the COVID-19 pandemic.

Possessing about 20 million users in 2020, Microsoft 365 has since grown to over 430 million paid commercial users worldwide.[2] Further, the estimated number of active monthly Microsoft Teams users now exceeds 300 million. Microsoft Teams especially has had great success in enterprises, where 93% of Fortune 100 companies utilize it for communications.[3]

Having an established foothold in organizations of all sizes, Microsoft has already taken steps to strengthen its presence in them. Two specific Microsoft 365 features that more midmarket enterprises utilize include:

- ***Microsoft Entra.*** Formerly known as Azure Active Directory, Microsoft Entra serves as the foundational identity management platform within Microsoft 365. It provides baseline security services such as single sign-on (SSO), multi-factor authentication (MFA), and user governance. It also provides more advanced services such as managing and securing AI agents that access enterprise resources.[4]
- ***Microsoft Power Platform.*** Centralizing and consolidating applications and data in Microsoft 365 create opportunities for midmarket enterprises to improve internal work processes. Microsoft Power Platform tools, such as Power Automate and Power BI, equip them to automate workflows and visualize their data.

  Microsoft Copilot, Microsoft 365's built-in artificial intelligence (AI) tool, serves as the backbone for the Microsoft Power Platform. Copilot performs tasks ranging from writing emails to summarizing reports to providing deeper insights into existing data.

  Since Copilot also accesses information within a midmarket enterprise's Microsoft 365 data repository, it provides specific insights germane to that enterprise. These capabilities have already prompted more organizations to deploy Copilot company-wide.[5]

This combination of midmarket enterprises utilizing Microsoft 365's existing functionality and adoption of new features highlights Microsoft 365's entrenchment in them. Microsoft 365's existing features have already impacted how individuals within midmarket enterprises communicate and interact with one another. Its new features further enhance how they manage and secure their data, gain insights into it, and automate repetitive or mundane tasks.

Yet as more midmarket enterprises embrace Microsoft 365, they must account for how they will protect data stored in it. This task becomes ever more complex as midmarket enterprises utilize Microsoft 365's existing and new features.

They must minimally establish how third-party Microsoft 365 software-as-a-service (SaaS) backup solutions protect Exchange, OneDrive, SharePoint, and Teams. Midmarket enterprises adopting Entra and Power Platform should also consider protecting their data hosted in these offerings as well.

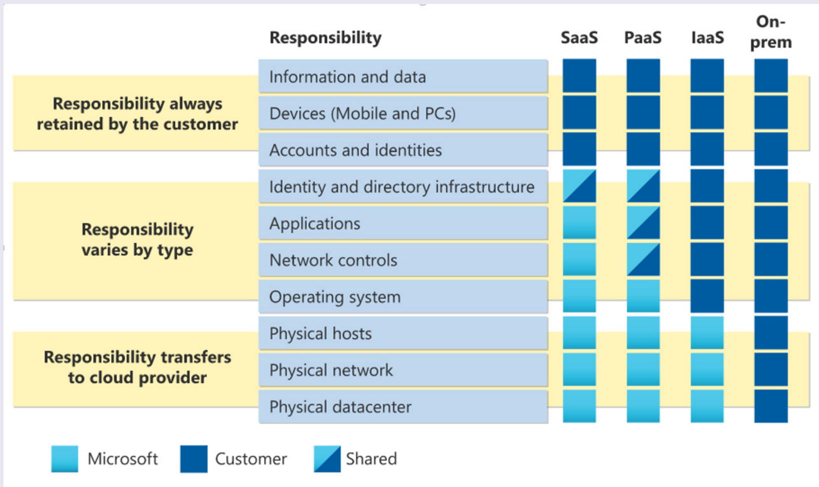
Support for backing up data in these new Microsoft 365 options remains nascent. Concerned midmarket enterprises should therefore consider the roadmap a provider has for protecting data in these new Microsoft 365 features.

Cloud-based, third-party Microsoft 365 SaaS backup solutions often provide the best option for midmarket enterprises to perform holistic backup and recovery.

Data Stored in Microsoft 365 Remains Your Responsibility

Midmarket enterprises adopt Microsoft 365 largely driven by the business value that Microsoft 365 delivers. They gain access to Exchange, OneDrive, SharePoint, and Teams while alleviating themselves of the tasks associated with hosting Microsoft 365. However, one responsibility remains with midmarket enterprises.

They retain the responsibility to protect the data and user identity information that they store in Microsoft 365. While many organizations now understand this responsibility, up to 30 percent may still not have a backup strategy in place.[6]



	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	■	■	■	■
	Devices (Mobile and PCs)	■	■	■	■
	Accounts and identities	■	■	■	■
Responsibility varies by type	Identity and directory infrastructure	◩	◩	■	■
	Applications	□	◩	■	■
	Network controls	□	◩	■	■
	Operating system	□	□	■	■
Responsibility transfers to cloud provider	Physical hosts	□	□	□	■
	Physical network	□	□	□	■
	Physical datacenter	□	□	□	■

□ Microsoft ■ Customer ◩ Shared

Source: Microsoft [7]

Microsoft does use terms such as data availability and protection when discussing Microsoft 365's features. However, midmarket enterprises should view these references primarily in the context of high availability (HA) and data security. For instance, Microsoft hosts Microsoft 365 in highly available Microsoft Azure data centers. Further, Microsoft physically secures these data centers and employs antivirus and firewall software to protect data from attacks.

Microsoft 365 even offers some limited data protection capabilities. Its Deleted Items and Recycle Bin utilities retain recently deleted data, and permit restores of deleted emails and files.

However, midmarket enterprises should not equate these two utilities with backup software that holistically protects data stored in Microsoft 365. Cloud-based, third-party Microsoft 365 SaaS backup solutions often provide the best option for midmarket enterprises to perform holistic backup and recovery.

The State of Microsoft 365 SaaS Backup Solutions

Microsoft 365 SaaS backup solutions have continued to mature and improve significantly since DCIG last evaluated them in 2023. Further, midmarket enterprises have more Microsoft 365 SaaS backup solutions from which to choose, with over 20 available offerings.

Many of the benefits of these Microsoft 365 SaaS backup solutions remain unchanged from DCIG's last evaluations. Examples of the benefits that most of these solutions continue to offer include:

- Backup Microsoft Exchange, OneDrive, SharePoint, and Teams
- Encrypt Microsoft 365 backups.
- Free trial periods (typically 15 – 30 days)

- May subscribe online to the solution.
- May immediately schedule backups of Microsoft 365 data.
- Provider handles all back-of-house administrative tasks associated with hosting its solution. These tasks include hosting and scaling the solution as well as performing ongoing software fixes, patches, and updates, among other jobs.
- Store backups on cloud object storage from one or more cloud providers.

However, other features have changed and matured. These include the following.

To ensure all Microsoft 365 user data gets protected, many Microsoft 365 SaaS backup solutions can adapt to changes in Microsoft 365.

Billing

Microsoft 365 SaaS backup solutions typically assess charges based on the following two components: a per-user fee and backup storage consumption. The per-user fee correlates to the number of Microsoft 365 licenses that an enterprise has.

To ensure all Microsoft 365 user data gets protected, many Microsoft 365 SaaS backup solutions can adapt to changes in Microsoft 365. As the number of Microsoft 365 users increases or decreases, the SaaS backup solution may dynamically increase or decrease its number of licenses.

Many providers also charge fees for backup storage costs, though how they charge varies by provider. Some calculate storage costs based on the total amount of backup data stored on the backend storage devices. Others calculate how much Microsoft 365 data they need to protect before they back it up. They then bill for storage based upon that calculated total.

Backing up Microsoft Teams

Support for Microsoft Teams across all Microsoft 365 SaaS backup solutions represents one notable difference since DCIG's last evaluation. While most solutions supported Microsoft Teams two years ago, all now back up Teams data.

Midmarket enterprises should still exercise caution when selecting a solution to protect Microsoft Teams. In the background, Microsoft Teams leverages SharePoint and OneDrive for specific Teams messaging and file sharing activities.

This approach results in Teams storing some messages and files in SharePoint and others in OneDrive. How well or even if a Microsoft 365 SaaS backup solution protects messages and files in both SharePoint and OneDrive varies.

Lack of support for Microsoft Teams did prompt DCIG to not formally evaluate one new Microsoft 365 SaaS backup solution, Microsoft 365 Backup. A notable entrant into the backup space, Microsoft 365 Backup currently only backs up Exchange, OneDrive, and SharePoint.[8]

DCIG views support for Teams backup as critical to a comprehensive Microsoft 365 backup solution. Currently, only third-party Microsoft 365 backup solutions, such as DCIG evaluated, offer this functionality.

Backup Storage Targets

Microsoft 365 SaaS backup solutions manage the underlying storage on which the backups reside, often providing a default storage option. However, some offer options on where to store their Microsoft 365 backups with choices varying between backup solutions. Consider:

- Some only store backups in the provider's cloud.
- Others give enterprises a choice of cloud storage targets from one or more providers.
- Some can place or tier backups based on cost, location, or performance characteristics.
- A few offer the option to use an enterprise's on-premises storage.

Once configured, midmarket enterprises rarely need to have concerns about sufficient storage capacity for their backups. However, midmarket enterprises that must meet specific budgets or recovery requirements should select solutions that give them control over where they place their backups.

Cyber Resilience

Cyber resilience in Microsoft 365 SaaS backup solutions has gone from an afterthought to a core component across all solutions. Cyber resilience may show up in any of the following ways in these solutions:

- Anomaly detection.
- Data encryption
- Data immutability.
- Data loss prevention
- Ransomware detection.

Cyber resilience in Microsoft 365 SaaS backup solutions has gone from an afterthought to a core component across all solutions.

Anomaly and ransomware detection have received the most attention from these providers over the last two years. This stems in large part from Microsoft 365 being the most common way that bad actors attempt to infiltrate midmarket enterprises.

To detect anomalies and ransomware, many providers have introduced artificial intelligence (AI) into their respective solutions. However, their detection capabilities vary widely, with each one using different algorithms and techniques to identify anomalies and ransomware. Many also use AI for data loss prevention to limit and stop sensitive data from leaving the organization.

Responses to detected or suspected anomalies or instances of ransomware also vary. Some merely send out alerts that they have detected a threat. Others take more proactive steps, such as quarantining specific users or instances after identifying a threat. Some solutions can even recover an affected file or message without any intervention by a user or administrator.

Data encryption and immutability come into play to protect backups. Many Microsoft 365 SaaS backup solutions utilize the Cloud Lock feature available on cloud object storage. This prevents ransomware from changing, deleting, or encrypting already stored backups during an attack. All providers can also encrypt backups, which makes backups unreadable to bad actors should they obtain a copy of the backup.

SaaS Backup Hosting

All SaaS backup solution providers host their respective solution in a highly available data center. However, the cloud data center each provider uses varies by provider. Consider:

- Over half of the providers can host their solution with a third-party cloud provider such as Amazon Web Services (AWS) or Google Cloud Platform (GCP).
- Approximately half of the evaluated solutions can host their SaaS backup solution in Microsoft Azure.
- Another third can host their solution in a purpose-built cloud that the provider owns or leases.

While greater than 100 percent of the total, it stems from some providers hosting their solution in multiple clouds. Some midmarket enterprises may want this flexibility for different reasons. Some may already use a specific cloud (AWS, Azure, or GCP). Still others may prefer a purpose-built cloud as it offers more predictable cloud costs and defined disaster recovery (DR) options. Regardless of the solution, the provider often includes a service level agreement (SLA) of 99.5% or greater for high availability.

Spanning Backup for Microsoft 365

Spanning Backup for Microsoft 365

Spanning built Backup for Microsoft 365 on multiple AWS services and continues to host it in AWS.[8] Using Backup for Microsoft 365, midmarket enterprises can both automate daily backups and perform on-demand backups. Further, Spanning guarantees reliable restores and backs this guarantee with a 99.9% service level agreement (SLA).[9]

Midmarket enterprises may also find Spanning's premium Dark Web Monitoring appealing. Dark Web Monitoring monitors and scans tenant domains for data breach records collected by its dark web monitoring services. It then notifies the Spanning administrator should it identify any potentially compromised user credentials.[10] In addition to Microsoft 365, Spanning can protect data residing in Google Workspace and Salesforce.

> ***Spanning relies upon AWS and leverages many of the features inherently available in AWS to automate and simplify Backup for Microsoft 365's ongoing management.***

Other features that help distinguish Spanning Backup for Microsoft 365 from other TOP 5 solutions include:

- ***Admins cross-user restores.*** Administrators may restore data from one user's backup to any other user's Microsoft 365 account. Midmarket enterprises most often use this feature to address processes like employee offboarding *(e.g., transferring emails or OneDrive files to a manager after termination)* or migrations *(e.g., moving data to a new user during reorganizations)*.[11]

- ***Leverages AWS' capabilities to automate management of Backup for Microsoft 365.*** Spanning relies upon AWS as its sole public cloud infrastructure. In so doing, it leverages many of the features inherently available in AWS to automate and simplify Backup for Microsoft 365's ongoing management. For instance, it utilizes different AWS EC2 instances to perform backup, restore, export, and search functions. Each of these roles then has its own AutoScale group assigned to it. They then scale up or down based upon their associated Amazon CloudWatch metrics.[12]

- ***Immutable audit logs.*** Spanning includes immutable, tamper-proof audit logs of all backup and restore activities. These logs ensure transparency and compliance with regulatory requirements. They track every action (e.g., backup failures, deletions, restores, etc.,) that regulated industries often must produce during audits.[13]

- ***Regional data centers to meet data sovereignty requirements.*** Midmarket enterprises may choose from AWS cloud data centers in specific geographic regions. These include the US, Canada, EU, UK, South Africa, and Asia Pacific (Australia) to comply with various data residency and sovereignty regulations. Spanning Admins select from among these regions during setup.[14] However, Spanning Admins may need to manually verify that the selected region complies with the regulations in question. ■

Sources

1. https://www.microsoft.com/en-us/microsoft-365-life-hacks/stories/looking-back-ten-years-microsoft-365. Referenced 8/4/2025.
2. https://view.officeapps.live.com/op/view.aspx?src=https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/TranscriptFY25Q3. Referenced 8/5/2025.
3. https://www.businessofapps.com/data/microsoft-teams-statistics/. Referenced 8/5/2025.
4. https://www.microsoft.com/en-us/security/business/microsoft-entra. Referenced 8/5/2025.
5. seekingalpha.com/article/4806519-microsoft-corporation-msft-q4-2025-earnings-call-transcript. Referenced 8/5/2025.
6. https://thehackernews.com/2025/01/insights-from-2025-saas-backup-and-recovery-report.html Referenced 8/6/2025.
7. https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility. Referenced 8/6/2025.
8. https://www.spanning.com/blog/effective-engineering-in-the-cloud-using-aws-for-product-growth/. Referenced 9/3/2025.
9. https://appsource.microsoft.com/en-us/product/saas/spanningcloudappsllc.spanningbackupforoffice365. Referenced 9/3/2025.
10. https://help.spanning.kaseya.com/help/Content/K-Span-365/dark-web.htm. Referenced 9/3/2025.
11. https://appsource.microsoft.com/en-us/product/saas/spanningcloudappsllc.spanningbackupforoffice365, Referenced 8/27/2025.
12. https://www.spanning.com/blog/effective-engineering-in-the-cloud-using-aws-for-product-growth/. Referenced 9/3/2025.
13. https://spanning.com/blog/new-restore-options-admin-audit-log/, Referenced 8/27/2025.
14. https://www.spanning.com/spanning-global-data-centers/. Referenced 8/27/2025.

About DCIG

The Data Center Intelligence Group (DCIG) empowers the IT industry with actionable analysis. DCIG analysts provide informed third-party analysis of various cloud, data protection, and data storage technologies. DCIG independently develops licensed content in the form of DCIG TOP 5 Reports and Solution Profiles. Please visit **www.dcig.com.**