Solution Profile

2025-26 DCIG TOP 5

MICROSOFT 365 SAAS BACKUP SOLUTIONS // SMB EDITION

Datto SaaS Protection+

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 // SMB Edition

Datto SaaS Protection+

SOLUTION

Datto SaaS Protection+

COMPANY

Kaseya
701 Brickell Ave #400
Miami, FL 33131
(888) 294-6312
datto.com

DISTINGUISHING FEATURES OF DATTO SAAS PROTECTION+

- Automatically performs user backups 3x daily.
- Private Datto cloud data centers in Australia, Canada, Germany, Singapore, UK, & US.
- Replicates all data to other data centers in same region.
- Restores to a different location to avoid overwriting current content.
- Scans Microsoft 365 backups for signs of malware and phishing.
- Uses four designations to classify successful backups.

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 organizations, 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 small and midsized businesses (SMBs) 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 SMB resources.[4]
- ***Microsoft Power Platform.*** Centralizing and consolidating applications and data in Microsoft 365 create opportunities for SMBs 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 an SMB's Microsoft 365 data repository, it provides specific insights germane to that SMB. These capabilities have already prompted more organizations to deploy Copilot company-wide.[5]

This combination of SMBs 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 SMBs 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 SMBs embrace Microsoft 365, they must account for how they will protect data stored in it. This task becomes ever more complex as SMBs 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. SMBs adopting Entra and Power Platform should also consider protecting their data hosted in these offerings as well.

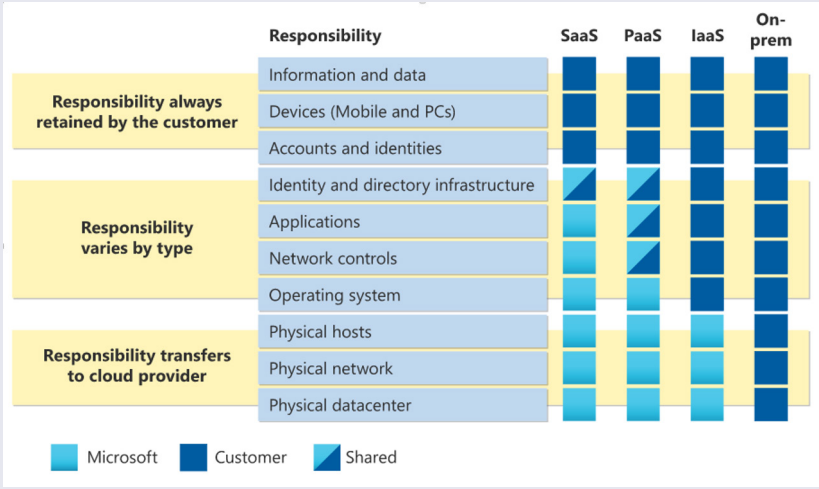
Support for backing up data in these new Microsoft 365 options remains nascent. Concerned SMBs should therefore consider the roadmap a provider has for protecting data in these new Microsoft 365 features.

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

Data Stored in Microsoft 365 Remains Your Responsibility

SMBs 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 SMBs.

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]



Source: Microsoft [7]

Microsoft does use terms such as data availability and protection when discussing Microsoft 365's features. However, SMBs 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, SMBs 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 SMBs 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, SMBs 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 evaluated them. 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 SMB 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.

SMBs 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 SMBs a choice of cloud storage targets from one or more providers.
- Some can place or tier backups based on cost, location, or performance characteristics.

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

Datto SaaS Protection+

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

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:

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

Ransomware detection and data preservation have received the most attention from these providers in recent years. This stems in large part from Microsoft 365 being the most common way that bad actors attempt to infiltrate SMBs.

To detect ransomware, some providers utilize anti-malware software in their respective solutions. However, their detection capabilities vary widely, with each one using different algorithms and techniques to identify ransomware.

Data encryption and immutability have also come into play to protect backups. Some 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 SMBs may want this flexibility for different reasons. Some may already use a specific cloud (AWS or Azure). 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.

Datto SaaS Protection+

Datto, a Kaseya company, hosts SaaS Protection and its backups in multiple Datto private cloud data centers. These locations span Australia, Canada, Germany, Singapore, the United Kingdom (UK) and the United States (US). At each data center Datto offers built-in redundancy and high availability. It then also replicates all data to other data centers in the same geographical region.

Datto automatically performs user backups three times daily retaining them for 30 days. After 30 days, it saves one daily backup per user and, after 90 days, it saves one weekly backup per user. After one year, it saves one monthly user backup and then retains that backup indefinitely.[9]

To help SMBs better assess the status of a successful backup, Datto uses four designations to classify each one.

In addition to protecting Microsoft 365's four core services, Datto SaaS Protection protects Google WorkSpace. Other features that help distinguish Spanning Backup for Microsoft 365 from other TOP 5 solutions include:

- ***Provides additional insight into the status of successful backups.*** Like most Microsoft 365 SaaS backup solutions, Datto Saas Protection reports on overall backup failures and successes. However, just because Datto successfully completes a Microsoft 365 backup does not necessarily mean the backup completed issue-free.

  To help SMBs better assess the status of a successful backup, Datto uses four designations to classify each one. These include: (1) Successful; (2) Successful with a few issues; (3) Successful with issues; and (4) Successful with a lot of issues.[10]

- ***Restores to a different location to prevent overwriting current content.*** Datto SaaS Protection takes specific steps to avoid overwriting existing content when performing a restore any Microsoft 365 service. When restoring data, it creates a folder that contains at least one item at the root of the service. It then names the folder using the following naming convention: **SaaS Protection Restore YYYY-MM-DD HH:MM:SS**.

  SaaS Protection then may use an additional folder naming convention to help users find the restored data. For instance, in Exchange, if restoring data to Inbox, the folder it creates in Inbox has a number next to it. This number indicates the number of emails restored.[11]

- ***Scans Microsoft 365 backups for signs of malware infections and phishing.*** Datto SaaS Protection+ gets its name by combining Datto's SaaS Protection and SaaS Defense solutions. Unlike SaaS Protection, Datto hosts SaaS Defense in the Microsoft Azure cloud where Microsoft 365 also resides.

  By placing SaaS Defense in Azure, it can better detect threats as they occur in the production Microsoft 365 environment. SaaS Defense can identify malware, phishing, and ransomware as well as previously unidentified security threats. Should it identify a threat, its forensic analysis tool can investigate the threat and determine why the threat was blocked.[12] ■

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.microsoft.com/en-us/microsoft-365/microsoft-365-backup. Referenced 8/6/2025.
9. https://www.datto.com/wp-content/uploads/dlm_uploads/Datto-Product-Brief-Datto-SaaS-Protection-for-M365-2025.pdf. Pg. 4. Referenced 9/22/2025.
10. https://saasprotection.datto.com/help/M365/Content/Additional_resources/Release_notes.html. March 3, 2025, Release Notes. Referenced 9/22/2025.
11. https://saasprotection.datto.com/help/M365/Content/Recovering_and_restoring_files/01A_Data_restore_locations.htm. Referenced 9/23/2025.
12. https://saasdefense.datto.com/help/Content/About_SaaS_Defense/02_What_is_Datto_SaaS_Defense.htm. Referenced 9/22/2025.

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.**