Solution Profile

2023-24 DCIG TOP 5

SpinOne for Microsoft 365 Enterprise SaaS Backup Solution Profile

By DCIG Principal Data Protection Analyst, Jerome M Wendt

SpinOne for Microsoft 365 Enterprise SaaS Backup Solution Profile

Table of Contents

SpinOne for Microsoft 365 Enterprise SaaS Backup Solution Profile

SOLUTION

SpinOne for Microsoft 365

COMPANY

Spin.AI
2100 Geng Rd #210
Palo Alto, CA 94303
(888) 883-2993
spin.ai

DISTINGUISHING FEATURES OF SPINONE FOR MICROSOFT 365

- Monitors, audits, and controls access to Microsoft 365 data.
- Monitors Microsoft 365 for signs of ransomware and promptly counters attacks.
- Flexible storage location and user management.
- Support for multiple Microsoft 365 tenants.

DISTINGUISHING FEATURES OF TOP 5 MICROSOFT 365 ENTERPRISE SAAS BACKUP SOLUTIONS

- Annual billing.
- Automated daily backup with options to schedule multiple daily backups.
- Index backups.
- Integrate with SSO, MFA, and RBAC.
- Provide best options for protecting Microsoft Teams data.
- Securely erase deleted or expired data.
- Select and back up specific Microsoft Exchange, OneDrive, and SharePoint features.

SOLUTION FEATURES EVALUATED:

- *Anti-ransomware/cyber resilience.*
- *Backup administration and capabilities.*
- *Billing, configuration, and licensing.*
- *Recovery and restores.*
- *Support.*

Microsoft 365 Adoption Continues

DCIG's release of its inaugural TOP 5 Microsoft 365 (then Office 365) backup solutions report in 2021 coincided with the COVID-19 pandemic. During that outbreak enterprise adoption of Microsoft 365 grew by 15 percent year-over-year.[1] Further, the use of Microsoft Teams grew by more than 50 percent in one 6-month time span in 2020 alone.[2]

However, many states had stay-at-home directives in place in 2020 and 2021. This led to some questioning if Microsoft 365's growth would continue or possibly even regress once these restrictions eased.

Turns out, forecasts for Microsoft 365's continued growth beyond 2021 proved correct. By March 2023 the number of paid Microsoft 365 seats had increased to as high as 450 million.[3] These 220 million new seats, which includes commercial and consumer seats, represents nearly 96 percent growth in two years.

Microsoft Teams experienced even more explosive growth. By the end of March 2023, it had surpassed 300 million monthly active users.[4] This represents an increase of 185 million active users per month, or a 160 percent increase in that same time.

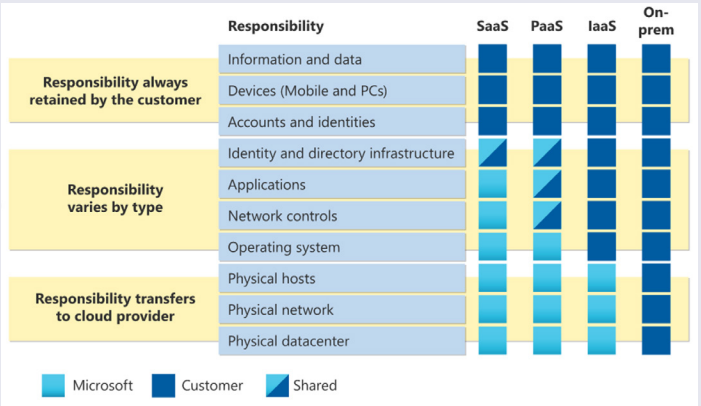
Microsoft has not yet shared statistics on adoption of other specific Microsoft 365 components. However, it reported that 80 percent of its enterprise customers use five or more Microsoft 365 applications.[5]

Microsoft 365's already large footprint may lead to slower growth in the future. To mitigate a slowdown in adoption, Microsoft plans to incorporate artificial intelligence (AI) throughout Microsoft 365 to improve user creativity and productivity. Microsoft has also announced TeamsPro, Teams Premium, and Viva as new Microsoft 365 applications.

Microsoft specifically refers to its new Microsoft 365 Viva application as a "super app" for sellers. Sellers may use Viva to capture, access, and register data in many Customer Relationship Management (CRM) systems.

Data Contained in Microsoft 365 Remains Your Responsibility

Microsoft 365's continued adoption reflects the value that enterprises derive from their adoption of Microsoft 365. They receive its benefits while alleviating themselves of many of its back-of-house administration tasks. However, one responsibility remains with enterprises. Data and user identity information that they store in Microsoft 365 remains their responsibility to protect.



Source: Microsoft[6]

Continued

SpinOne for Microsoft 365 Enterprise SaaS Backup Solution Profile

Microsoft may use terms such as data availability and protection when discussing Microsoft 365's features. However, enterprises should view these references primarily in the context of high availability (HA) and data security. For instance, Microsoft hosts Microsoft 365 in its highly available Azure data centers. It physically secures these data centers and employs antivirus and fire wall software to protect enterprise 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 the deleted emails and files.

However, enterprises should not equate these two utilities with backup software that holistically protects data stored in Microsoft 365. Cloud-based, software-as-a-service (SaaS) backup solutions provide the best data protection option for enterprises to perform Microsoft 365 backup and recovery.

Cloud-based, SaaS backup solutions provide the best data protection option for enterprises to perform Microsoft 365 backup and recovery.

The State of Microsoft 365 Enterprise SaaS Backup Solutions

Enterprises turn to Microsoft 365 SaaS backup solutions for multiple reasons. Chief among them, enterprises may quickly subscribe to these offerings. Once subscribed, they may often immediately perform backups of their data residing in Microsoft 365. These SaaS backup solution providers then handle all the back-of-house administrative tasks to include the backup software's ongoing fixes, patches, and updates.

Many of them also handle the management of the storage on which the backups reside. However, the storage management does vary between products. Some only direct backups to the storage in the provider's cloud. Others give enterprises a choice of storage targets, typically object storage, to include using an enterprise's on-premises storage. In either case, once they configure the storage, enterprises rarely need to worry about managing storage capacity for backups.

As their usage of Microsoft 365 increases or decreases, SaaS backup solutions can adapt to these changes, sometimes dynamically. This holds true for compute, storage, and even backup software user licenses. For instance, should an enterprise increase its number of Microsoft 365 licenses, the backup solution may automatically add more licenses. Should the number of licensed Microsoft 365 users decrease the backup solution may automatically decrease its number of licenses as well.

Enterprises will also find anti-ransomware, cyber resilience, or both these capabilities in all these backup solutions. They may support storing backups on immutable object storage, alert of suspected ransomware attacks, and quarantine infected files in backups.

Enterprises will find all evaluated SaaS backup solutions provide baseline data protection features for Microsoft 365. They protect data in the core Microsoft 365 applications that enterprises often use, such as Exchange, OneDrive, and SharePoint.

Teams, one of the newer Microsoft 365 applications, now is almost universally protected by all the evaluated solutions. In 2021 only about 50 percent of the backup solutions evaluated then protected Microsoft Teams in any fashion. Now all enterprise SaaS backup solutions that DCIG evaluated, with one exception, protects Teams.

All evaluated solutions deliver the foundational features that enterprises need to quickly begin protecting their Microsoft 365 data in the following ways. Consider:

SpinOne for Microsoft 365 Enterprise SaaS Backup Solution Profile

- ***Fast and affordable.*** Microsoft 365 SaaS backup solutions subscription services start at about US$4 per user per month with an annual contract. Once an enterprise subscribes and connects its Microsoft 365 tenant to the SaaS backup solution, backups often start automatically. Most solutions, by default, schedule initial and recurring Microsoft 365 backups with minimal or no administrative intervention.
- ***No installation, setup, or maintenance.*** Providers host their Microsoft 365 backup solution in either a general-purpose or purpose-built cloud. The solution providers then fix, patch, maintain, and update their software as part of their backup SaaS offering.
- ***Highly available.*** Each SaaS backup solution aligns with Microsoft 365 in an important way: it gets hosted in a highly available cloud. The cloud in which it gets hosted does vary. Some host their backup software in Microsoft Azure. Others use Amazon Web Services (AWS), Google Cloud Platform (GCP), or a purpose-built cloud. Regardless of the provider, they often include a service level agreement (SLA) of 99.5% or higher.
- ***Free trial periods.*** Enterprises may test a solution's backup and recovery capabilities through a free trial period. The providers typically limit the trial to about 30 days with the terms of each provider's trial period varying. The trial may include access to all features for some users; access to some features for all users; or some combination thereof.

SpinOne for Microsoft 365 Solution Profile

Upon DCIG's completion of reviewing nearly 30 available Microsoft 365 enterprise SaaS backup solutions, DCIG ranked SpinOne for Microsoft 365 as a TOP 5 solution. Spin.AI is the developer of the SpinOne platform which provides SaaS backup software that only protects data hosted in SaaS applications.

SpinOne distinguishes itself from competitors by performing cloud ransomware detection, preventing data leakage and loss, and supporting multiple cloud storage backup targets. SpinOne offers subscriptions to its Microsoft 365 Backup service with annual and department-level billing options. It also provides a trial period that includes access to all its features for a limited number of users.

SpinOne for Microsoft 365 includes Data Leak Prevention (DLP) capabilities that prevent access to sensitive information by unauthorized applications or individuals.

SpinOne for Microsoft 365 offers the following features that help distinguish it from other Microsoft 365 backup solutions.

- ***Monitors, audits, and controls access to Microsoft 365 data.*** Enterprises may send and/or store all types of sensitive information using Microsoft 365 Exchange, OneNote, SharePoint, and Teams. Personally Identifiable Information (identification documents, SSN, Passport Numbers, ITIN), medical records, or financial information (credit cards, bank accounts, statements, etc.) represent just some types of data individuals may send or store.

  Bad actors capitalize on this by configuring some malware strains to exfiltrate Microsoft 365 data. This could cause enterprises financial loss, violation of laws, regulations and contracts, and damage to business or individual reputation.

  SpinOne for Microsoft 365 includes Data Leak Prevention (DLP) capabilities that prevent access to sensitive information by unauthorized applications or individuals. Its SaaS Data Audit dashboard provides visibility into an enterprise's stored Microsoft 365 data.

  SpinOne performs data classification to identify files with sensitive information, and tracks users and applications that access this data. Through its SaaS Security Posture

SpinOne for Microsoft 365 Enterprise SaaS Backup Solution Profile

Management (SSPM) solution, SpinOne calculates risks of connected applications and extensions, and scores them. It uses these scores to allow or block application access to this data.[7]

- ***Monitors Microsoft 365 for signs of ransomware and promptly counters attacks if they occur.*** Recovering from a ransomware attack is good. Identifying and recovering from an in-progress attack before it has any impact is ideal. SpinOne complements traditional security stacks by also monitoring an enterprise's Microsoft 365 environment for any signs of ransomware.

  Should it detect ransomware, SpinOne performs four tasks within a two-hour SLA. First, it blocks the source of the ransomware. Second, it isolates the digital assets affected by the ransomware attack. Third, it restores any affected files to the more recent backed up version. Fourth, it notifies IT administrators of the attack and the steps it took to remedy it.[8]

- ***Offers flexible storage location and user management, along with support for multiple Microsoft 365 tenants.*** SpinOne for Microsoft 365 supports AWS, GCP, Azure, and bring-your-own-storage (BYOS) storage providers with multiple regions around the globe. Enterprises may configure backup retention domain wide, or per each Security Group to ensure compliance with internal policies. Enterprises may link multiple Microsoft 365 tenants together, to protect Google Workspace, Salesforce, and Slack data using one console. SpinOne may onboard, archive, or offboard users through its automated, configurable policies. ■

Sources

1. https://office365itpros.com/2020/10/28/teams-115-million-users/. Referenced 1/19/2021.
2. https://www.microsoft.com/en-us/Investor/earnings/FY-2021-Q1/press-release-webcast. https://www.microsoft.com/en-us/Investor/earnings/FY-2020-Q3/press-release-webcast. https://www.businessofapps.com/data/microsoft-teams-statistics/. Referenced 1/19/2021.
3. https://www.microsoft.com/en-us/investor/events/fy-2023/earnings-fy-2023-q3.aspx Referenced 5/2/2023.
4. Ibid.
5. Ibid.
6. https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility. Referenced 5/2/2023.
7. https://spin.ai/solutions/data-leak/. Referenced 4/6/2023.
8. https://spin.ai/solutions/cloud-ransomware/. Referenced 4/6/2023.