

2023-24 DCIG TOP 5



Afi.ai for Office 365 Enterprise SaaS Backup Solution Profile

By DCIG Principal Data Protection Analyst, Jerome M Wendt

Afi.ai for Office 365 Enterprise SaaS Backup Solution Profile

Table of Contents

- 3 Microsoft 365 Adoption Continues
- 3 Data Contained in Microsoft 365 Remains Your Responsibility
- 4 The State of Microsoft 365 Enterprise SaaS Backup Solutions
- 5 Afi.ai for Office 365 Solution Profile

Afi.ai for Office 365 Enterprise SaaS Backup Solution Profile



SOLUTION

Afi.ai for Office 365

COMPANY

Afi.ai
 210 N. University Drive, #303
 Coral Springs, FL 33071
 (404) 946-6052
 afi.ai

DISTINGUISHING FEATURES OF AFI.AI FOR OFFICE 365

- Preemptive Microsoft 365 backup should Afi detect a ransomware attack.
- Flexibility to use any encryption key management service (KMS).
- Granular Microsoft Exchange search and restoration features.

DISTINGUISHING FEATURES OF 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 active monthly users.⁴ This represents an increase of 185 million active users per month, or a 160 percent increase in that same time.

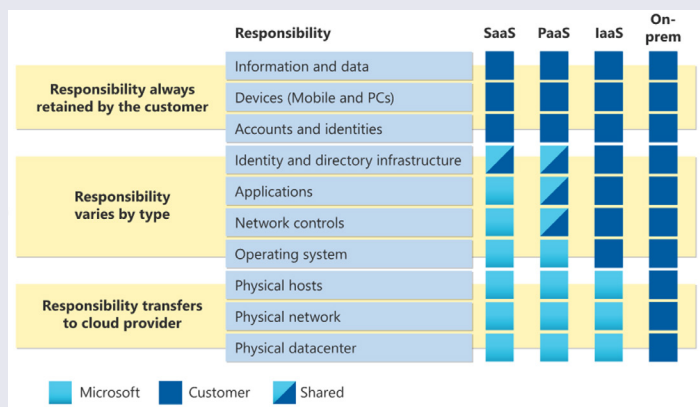
Microsoft has not yet shared statistics on adoption of other specific Microsoft 365 components. However, it reported that 80 percent of its enterprise customers use five or more Microsoft 365 applications.⁵

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®

Continued

Afi.ai for Office 365 Enterprise SaaS Backup Solution Profile

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

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.

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:

Afi.ai for Office 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.

Afi.ai for Office 365 Solution Profile

Upon DCIG's completion of reviewing nearly 30 available Microsoft 365 enterprise SaaS backup solutions, DCIG ranked Afi.ai for Office 365 as a TOP 5 solution. Afi as a company provides SaaS backup software that exclusively focuses on protecting data stored in SaaS applications.

Afi distinguishes itself from competitive offerings by including advanced management, recovery, search, and security capabilities in its software. Afi for Office 365 SaaS Backup offers subscriptions to its backup service with multiple different billing options. It also offers a 30-day trial period that includes access to all its features for an unlimited number of users.

Afi for Office 365 SaaS Backup offers the following features that help distinguish it from other Microsoft 365 backup solutions.

- **Preemptive Microsoft 365 backup should Afi detect a ransomware attack.** Afi brings its advanced capabilities in backup and security together to mitigate the impact of a ransomware attack. Afi's security features use its built-in artificial intelligence and Microsoft 365's APIs to monitor Microsoft 365 for uncharacteristic behaviors. These may include activities such as deletions or encryptions typical of ransomware attacks. Should it detect these occurrences it immediately performs two tasks. It notifies administrators of a possible attack and creates an immutable backup of production Microsoft 365 data. The timing of this backup ensures enterprises have a near realtime recovery point.
- **Flexibility to use any encryption key management service (KMS).** Whether enterprises store their Microsoft 365 backups on cloud storage or on-premises, this practice almost dictates they encrypt the backups. Encrypting backups also necessitates that an enterprise utilizes a KMS to encrypt and decrypt them. Afi provides enterprises the flexibility to use any available KMS, such as Amazon KMS or Azure Key Vault. By retaining controlling of the KMS, enterprises may withdraw the encryption key thereby making backups stored in the cloud inaccessible.

Afi's security features use its built-in artificial intelligence and Microsoft 365's APIs to monitor Microsoft 365 for uncharacteristic behaviors.

Afi.ai for Office 365 Enterprise SaaS Backup Solution Profile

- **Granular Microsoft Exchange, SharePoint, and Teams search and restoration features.** Restoring individual items (emails, folders, mailboxes) in Exchange represents a common task that backup administrators perform. To accelerate and simplify this task, Afi offers granular search and restoration features. To assist in finding specific emails to recover, Afi indexes all emails it backs up. Enterprises may then perform full text searches to find emails based on either the email's content or its metadata. To accelerate restores, Afi also makes it possible for enterprises to grant individuals to access their backups and restore their emails. Enterprises may enable this self-recovery option on a user-by-user basis. ■

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.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.

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.



DCIG, LLC // 7511 MADISON STREET // OMAHA NE 68127 // 844.324.4552

dcig.com

© 2023 DCIG, LLC. All rights reserved. Other trademarks appearing in this document are the property of their respective owners. This DCIG report is a product of DCIG, LLC. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. Product information was compiled from both publicly available and vendor-provided resources. While DCIG has attempted to verify that product information is correct and complete, feature support can change and is subject to interpretation. All features represent the opinion of DCIG. DCIG cannot be held responsible for any errors that may appear.

Licensed to Afi.ai with unlimited, unrestricted global distribution rights.

May 2023 6