

Make the Best Choice between Afi and Backupify for Microsoft 365 Backup and Recovery

by DCIG President & Founder, Jerome M Wendt

PRODUCTS

Afi SaaS Backup

URL ► <https://afi.ai/>

Afi
210 N University Dr, Suite 303
Coral Springs, FL 33071
(404) 946-6052

Backupify/Datto SaaS Protection (“Backupify”)

URL ► <https://www.backupify.com/>

Backupify, a Datto Company
50 Milk Street, Suite 1300
Boston, MA 02109
(800) 571-4984

USE CASE

Enterprises with hundreds to tens of thousands of users that must protect their production data stored in Microsoft 365.

Microsoft 365: Your Data, Your Responsibility

Many enterprises already use Microsoft Office 365 for Enterprise as their default office productivity software solution. Using this software results in them storing increasing amounts of their data with these providers. Unfortunately, enterprises may overlook the need to protect this data from threats such as ransomware and user error.

Microsoft only takes responsibility for the infrastructure it uses to deliver its cloud software services. It also limits responsibility for the protection of data that enterprises host with it. Microsoft Services Agreement states, *“Your Content remains Your Content and you are responsible for it.”*¹

Data backup and recovery remains the responsibility of enterprises. To protect this data, enterprises will want to use an independent, cloud-based backup-as-a-service (BaaS).

Afi SaaS Platform and Backupify

The Afi SaaS Platform and Backupify each deliver enterprise, cloud-based BaaS solutions. They each protect Microsoft 365 and only require that enterprises subscribe to their respective service to back up data.

Both these solutions back up and recover core Microsoft 365 components (Exchange, OneDrive, SharePoint, and Teams.) However, differences exist in how they deliver on at least four of their respective backup and recovery capabilities. These include:

- Access control and management
- Anti-ransomware capabilities
- Completeness of backup capabilities
- Completeness of recovery capabilities

#1: Access Control and Management

Enterprises require BaaS solutions to deliver a comprehensive identity and access management (IAM) offering to effectively use them. A BaaS solution should ideally address the following elements:

- Encryption key management
- Single sign-on
- Self-service end user recoveries
- Granular administrative access permissions

Encryption Key Management

Both Afi and Backupify encrypt backup data at-rest and in-transit using AES-256 encryption. In this way both secure backup data from either accidental or malicious access. However, they take different approaches to managing the keys used to encrypt the data.

The Afi SaaS Platform permits organizations to use any key management service (KMS). This frees organizations to use solutions such as Amazon KMS, Azure Key Vault, and Google Cloud KMS from leading cloud providers.

Enterprises with over 10,000 employees want this flexibility. They need total control over all their data to include management of their encryption keys. By using any of these KMS solutions, enterprises retain control. Should they need to make Microsoft 365 backup data stored in the cloud inaccessible, they may withdraw the encryption key.

Single Sign-on (SSO)

Enterprises increasingly use SSO solutions to simplify and accelerate user access to enterprise applications. Cloud providers such as Google, Microsoft, and Okta offer SaaS-based SSO solutions. These providers make it easier for enterprises to subscribe to and implement SSO.

The Afi SaaS Platform incorporates the availability of these SSO solutions into its design. Afi only grants users access to its platform after they get authenticated and authorized by an SSO provider. Afi uses SSO solutions from Google, Microsoft, and Okta.

Backupify also integrates with and supports SSO from multiple different SSO cloud providers. However, Backupify does separately permit administrators to access its console using their Microsoft 365 email address and password.²

Self-service End User Recoveries

All organization, regardless of its size, will eventually need to recover data. Many of these requests will originate from end-users who accidentally delete their data. Unfortunately, the more employees an organization has, the more frequently these events occur.

Afi grants end users access to their backups to perform self-service restores. Afi allows administrators to enable or disable this option and configure

1. <https://www.microsoft.com/en-us/servicesagreement>. 8/4/2020.

2. <https://help.datto.com/s/article/KB2048066041>. Referenced 4/8/2021.

permitted self-service operations. This positions organizations to reduce the support load of their IT staff by having end users perform their own recoveries.

In Backupify's case, only its administrators may restore data for individual Microsoft 365 end users.³

Granular Administrative Access Permissions

Organizations with large IT teams need multiple roles to administer their Microsoft 365 SaaS backup solution.

The Afi SaaS Platform offers multiple backup administrator roles. Each role offers different levels of access and views into the backup data. Organizations may then granularly control the level of visibility each role has into the data. Organizations may also set permissions that establish the actions each role can perform on the data. (Figure 1.)

Afi Office 365 Admin Options

SLA	Info	Apps	Roles & Self-Service
Admin			
			Access to users data <input checked="" type="checkbox"/>
			Preview email content <input checked="" type="checkbox"/>
			Download data <input checked="" type="checkbox"/>
Backup Operator			
			Configure SLA and initiate backup <input checked="" type="checkbox"/> Manage accounts
			Access to users data <input checked="" type="checkbox"/>
			Preview email content <input checked="" type="checkbox"/>
			Download data from backup <input checked="" type="checkbox"/>
			Recover to another folder <input checked="" type="checkbox"/>
			Recover with overwrite option <input checked="" type="checkbox"/>
			Recover to another account <input checked="" type="checkbox"/>
Self Service			
			Self-service for non-admin accounts <input checked="" type="checkbox"/>
			Access to users data <input checked="" type="checkbox"/>
			Download data <input checked="" type="checkbox"/>
			Recover to another folder <input checked="" type="checkbox"/>

Figure 1 Source: Afi

In contrast, Backupify offers only two administrator roles, Super Administrator and Admin, with no options to customize the permissions. Only one Super Administrator role exists per account with this role assigned to the email provided during account registration.⁴ Members of the Admin account all have the same level of access to Microsoft 365 user data for backups and restores. This includes read, write, and view access to user data across all Microsoft 365 components (Exchange, OneDrive, etc.)⁵

Management and Account Navigation

Afi leverages the Azure Active Directory (AAD) structure to automate backup management and account navigation in large Microsoft 365

3. <https://help.datto.com/s/article/KB2050174901>. Referenced 4/28/2021.
 4. <https://help.datto.com/s/article/KB3600389269921>. Referenced 4/29/2021.
 5. <https://help.datto.com/s/article/KB370000000001>. Referenced 4/29/2021.
 6. <https://www.mystateline.com/news/local-news/winnebago-county-it-experts-talk-cyber-security-amid-rps-breach/>. 7/21/2020.
 7. <https://compliance-group.com/average-ransomware-payment-amount-increases-in-2019/>. 7/21/2020.

domains. Backup administrators may browse domain resources using AAD group structure and assign protection based on user group membership. (Figure 2.)

Afi AAD Group Interface

AAD Groups			Resources	SLA
<input checked="" type="checkbox"/>	Argentina Marketing Team	6		Not Protected
<input type="checkbox"/>	Executives	0		Not Protected
<input type="checkbox"/>	G1	9		Not Protected
<input type="checkbox"/>	Super Team	17		Not Protected
All resources				
<input type="checkbox"/>	Users	22		Gold
<input type="checkbox"/>	Sites	10		Gold
<input type="checkbox"/>	Office 365 Groups & Teams	3		Not Protected
<input type="checkbox"/>	Shared Mailboxes	0		Not Protected
<input type="checkbox"/>	Rooms & Equipment	0		Not Protected

Figure 2 Source: Afi

CHART 1

IAM Features

	Afi SaaS Platform	Backupify
Encryption Key Mgmt	Any KMS Provider	LUKS*
Sign-on	Multiple SaaS SSO Providers, including Okta SAML	Multiple SaaS SSO Providers Email + Password
End User Self Recovery	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Admin Roles	Administrator Backup Operator	One Super Admin Administrator
Admin Role Definitions	<input checked="" type="checkbox"/>	<input type="checkbox"/>

* Linux Unified Key Setup Supported Undetermined/Unsupported

KEY QUESTIONS TO ASK

- Do you want or need the option to control the encryption keys assigned to your Microsoft 365 backup data?
- How important is it to control and authenticate each user's sign-on to the backup solution?
- Do you want to grant end-users the ability to perform their own recoveries?
- Do you need to create multiple backup administrator roles with different responsibilities?

#2: Anti-ransomware Capabilities

Ransomware represents a growing threat to all size organizations. One estimate put the average cost per incident at over \$8 million with each one requiring 287 days to recover.⁶ Ransomware payment amounts average above \$40,000 with enterprises paying in excess of \$1 million per incident.⁷

These payouts only encourage hackers to develop more sophisticated ransomware making a ransomware attack an almost inevitable occurrence. Organizations should plan on when, not if, a ransomware attack occurs. Early detection, good, reliable backups, and fast restores in the event of an attack provide the keys to recovery.

Afi AI Engine and Preemptive Backups

The Afi SaaS Platform continually monitors changes to production Microsoft 365 data. Afi's built-in artificial intelligence uses Microsoft 365 APIs to monitor for abnormal changes to the data, such as encryption activity. Should it detect this type of activity, it immediately issues a warning and takes a preemptive backup for the entire account.

The incremental backups only take seconds or minutes to complete. Since a ransomware attack may take hours or even days to encrypt the data, Afi's preemptive backup mitigates the impact of the ransomware attack. Once the backup completes, Afi auto-labels it as the most recent, clean backup prior to the attack. Afi then further protects this and all its backups by storing them in an immutable, encrypted format in a public cloud.

Once immutably stored, Afi mitigates unauthorized access, deletions, or modifications to the backup data. Administrators cannot individually delete or modify the data. Requests must be made by creating a support ticket. Once submitted, a support specialist asks verification questions and may require a second person to authorize the request.

Finally, Afi helps organizations perform a root cause analysis to determine the source of ransomware attack. To do so, it maintains an immutable audit log that captures WAN IP addresses in the audit log. This log contains multiple details to include admin account names, data exports, operation details, and timestamps, among others. Organizations may optionally review this log to identify rogue actions by administrators or users.

Backupify

Backupify helps prevent against ransomware in the following ways. It stores Microsoft 365 backup data in its own private cloud, the Datto Cloud. This approach creates an air gap between the production data stored in the Microsoft Azure cloud and the Datto Cloud.

To help detect and prevent ransomware attacks, Backupify recommends organizations deploy a separate anti-ransomware solution: Vade Secure for Office 365. Vade Secure protects against malware, phishing, and spear-phishing attacks. Activating Vade Secure requires organizations to subscribe to it apart from their Backupify subscription.⁸

KEY QUESTIONS TO ASK

- Do you want or need an up-to-the-minute backup should a ransomware attack occur?
- Do you want or need to restrict administrative access to your backup data?
- Do you need an immutable audit log of activity in Microsoft 365 environment?
- Do you want or need to keep your backup data stored in an immutable format in a public cloud?

CHART 2

Anti-ransomware Capabilities

	Afi SaaS Platform	Backupify
Preemptive Backups		
Cloud Storage Target	Azure Google Cloud	Datto Cloud
Immutable Cloud Storage		
Anti-ransomware Software	Native	Vade Secure for Office 365
Immutable Audit Log		
Restricted Admin Access to Backup Data		

Supported Undetermined/Unsupported

#3: Completeness of Microsoft 365 Backup Capabilities

Microsoft 365 has four primary components in which organizations store data: Exchange, OneDrive, SharePoint, and Teams. Both the Afi SaaS Platform and Backupify protect data in all these components though they differ in the extent of support of new Microsoft 365 data sources.

Afi's Autonomous, Resilient Backups

Afi performs regularly scheduled backups and may also proactively initiate an out-of-schedule backup. It does so after examining multiple availability metrics that may affect an organization's Microsoft 365 account. For example, Afi looks at API latency, Microsoft cloud availability metrics, and news of disasters near datacenter locations, among others.

Should any of these items pose a threat, Afi initiates a complete data backup. During a natural disaster or a global cybersecurity event, Afi performs high frequency backups. These frequent backups result in autonomous, resilient Microsoft 365 protection to keep an organization's production Microsoft 365 data highly available.

In performing these Microsoft 365 backups, Afi comprehensively backs up each Microsoft 365 component. Consider:

- **Exchange.** Afi protects online archive, shared, and Teams mailboxes along with all the other common Exchange elements. Additionally, once it backs up Exchange emails, one may use Afi full-text-search to find emails. One may conduct searches based on metadata as well as content.
- **SharePoint.** Afi protects all SharePoint elements including SharePoint Lists, legacy and standard web pages.
- **Teams.** Afi backs up all Team data, to include new Teams data types such as Lists and Wiki pages. It protects both private and public Teams channels, including private channel data stored on a dedicated SharePoint site. Afi also protects Teams 1:1 conversations and their attachments. (Chart 3.)

8. <https://help.datto.com/s/article/KB360029616331>. Referenced 4/9/2021.

CHART 3

Granular Backup Options

	Afi SaaS Platform	Backupify
Backup Frequency	Continual Incremental Pre-emptive	3X daily Morning, Noon, & Night
Manual Full Backups	✔	✔
SharePoint Event Lists	✔	●
Threat Event Monitoring	✔	●
Proactive Full Backups (Threat detected)	✔	●

✔ Supported ● Undetermined/Unsupported

Backupify

Backupify similarly extends protection to all Microsoft 365 components and many of the features of each component. Backupify performs thrice daily backups which may occur at any time during each of the following windows:

- Midnight to 8 am, EST
- 8 am to 4 pm, EST
- 4 pm to 11:59 pm, EST

Should a backup fail, Backupify includes automated retry logic and has engineers on-call that monitor the backup environment.⁹

Backupify includes disclaimers about its Microsoft Teams and SharePoint data protection capabilities. It cannot back up private Teams Sites or private channel content. Organizations must use its SharePoint option to

back up private Teams Sites that exist in SharePoint. Even then, Backupify backs up that data without permissions.¹⁰

In SharePoint, Backupify does not currently back up any SharePoint Forms due to API limitations. Further, it cannot back up SharePoint image libraries or event lists.¹¹

KEY QUESTIONS TO ASK

- What amount of Microsoft 365 data loss, if any, is acceptable to your organization?
- Do you want or need your backup software to initiate backups if it detects a threat?
- Do you want or need your SharePoint and Teams data fully protected?

#4: Completeness of Recovery Capabilities

Afi and Backupify again differ in their completeness of abilities to recover Microsoft 365 data. While both solutions recover Microsoft 365 data, Afi provide deeper visibility into backup data and more granular restore options.

For example, Afi grants both administrators and end users the flexibility to securely access the Afi interface and restore their own data. In Backupify, only administrators may perform data restores.

When performing a restore, Afi provides previews into the content of backed up Microsoft 365 data. This view goes beyond file name or email subject metadata to reveal email and file contents. (Figure 3) This minimizes the need to guess which email or file to recover. Afi may also perform granular, permission-only restores for OneDrive files and folders.

SharePoint and Teams Granular Restores

Afi provides organizations with multiple options to perform different types of SharePoint restores. Both Afi and Backupify offer full restores of SharePoint Site backups, to include Document Libraries and Site Assets, Lists, Pages, and Templates.¹²

The differences emerge in the granularity of their respective restore options. Afi offers more detailed restore options for other SharePoint elements. Afi provides:

- **Automatic recovery of SharePoint Active Server Page Extended (aspx) files.** This eliminates the need for manual processes or the need to enable active scripting prior to recovering a SharePoint site.
- **Restores of a full List as well as selected items from within it.** Afi includes its online preview of List content with this granular recovery feature.
- **The option to recreate an entire SharePoint Site.** Afi enables the option to recover data from modern and classic SharePoint Sites.

If recovering Teams, Afi support supports full recoveries of Team content to an original Team or to a newly created one. If exporting Teams data, organizations may export it via either HTML or XML.

Since Afi supports both public and private Teams channels, it can recover both these types of Teams data. Backupify can only recover the portion of the Teams data stored in SharePoint.

Afi Recovery Console GUI

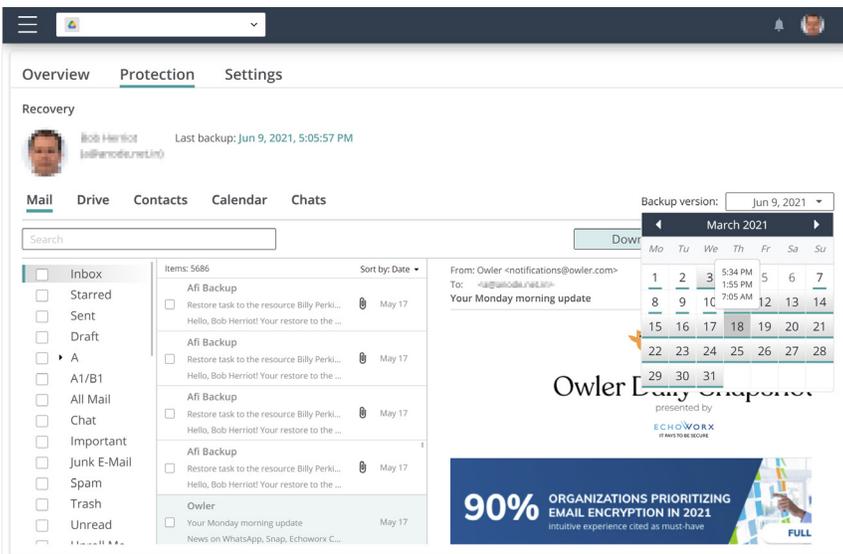


Figure 3

Source: Afi

Afi's Advanced Restore Capabilities

Afi further distinguishes itself from Backupify with a few advanced restore capabilities. For instance, if, and when, Afi detects a threat in the environment, it creates multiple backups and labels them. Should the threat impact the organization, it can quickly identify the optimal recovery points to accelerate recoveries.

Afi also represents one of the only BaaS solutions to provide a multi-channel natural language user interface (NLUI). Using Afi's NLUI, administrators or users may use email, messenger applications, or even the phone to request restores. Afi will authenticate and process this request and then automatically perform the restore. (Chart 4.)

KEY QUESTIONS TO ASK

- Do you want or need full backups automatically taken as soon as a potential threat is identified in your environment?
- Do you want the flexibility to perform restores without having to log into a backup console?
- Do you want or need more granular options to restore your SharePoint and Teams data? ■

CHART 4

Granular Recovery Options

	Afi SaaS Platform	Backupify
Restore Preview: Email/File Content	✔	●
Exchange Data File Export Options	EML, MBOX, PST	MBOX, PST ¹³
Labels Key Recovery Points	✔	●
NLUI	✔	●

* Natural Language User Interface.

✔ Supported ● Undetermined/Unsupported

13. <https://help.datto.com/s/article/KB1150021470261>. Referenced 5/1/2021.

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 TOP 5 Reports and Solution Profiles. More information is available at www.dcig.com.



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

dcig.com

© 2021 DCIG, LLC. All rights reserved. The DCIG Competitive Intelligence Report Executive Edition 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. No negative inferences should be drawn against any product or vendor not included in this report. DCIG cannot be held responsible for any errors that may appear. No negative inferences should be drawn against any vendor or product not included in this publication. This report was commissioned by Afi