IDC VENDOR SPOTLIGHT
Sponsored by: Afi

Enterprises rely on SaaS backup tools and services to bolster their data protection strategy by addressing compliance issues, data loss, security vulnerabilities, ransomware attacks, and business continuity risks.

Enterprise Data Growth and Adoption of Cloud Applications Challenge Traditional Data Protection Strategies

October 2021

Written by: Andrew Smith, Research Manager; Archana Venkatraman, Associate Research Director

Introduction

Cloud productivity and collaboration tools have become only more critical to businesses over the past year and a half as the ongoing challenges posed by COVID-19 have caused organizations to depend more on connecting remote workforces. Increased reliance on SaaS application suites such as Office 365 (O365), Salesforce, and Google Workspace is accompanied by data growth on these platforms and a potentially higher risk of data loss, security breaches, or service downtime.

Growing enterprise reliance on these application suites means that all organizations should have a backup and data protection strategy that goes above and beyond the baseline protection offered by the SaaS application provider natively. This will help organizations further ensure their data remains accessible, secure, and resilient within these platforms so they can be prepared to handle both planned and unplanned downtime.

Without a dedicated data protection strategy, organizations are exposing themselves to risks such as ransomware attacks, accidental data deletion, insider attacks, data loss, compliance issues, and data retention breaches. IDC research shows that more than 90% of organizations have been attacked by malware/ransomware and more than 80% have suffered a successful malware attack. Those that had been successfully attacked by ransomware cited significant consequences — direct loss of revenue, permanent loss of customers, lost employee productivity, IT personnel overtime, and loss of organizational reputation — not to mention the cost of the ransom if paid.

This analysis further details these threats and provides suggestions regarding how organizations should approach their Office 365 data protection strategies. Further, we assess Afi's solutions and explore the provider's strengths and key differentiators as well as some of the important opportunities and challenges associated with the SaaS data protection market.

AT A GLANCE

KEY STATS

- 60–70% of Microsoft 365 users rely on native/default backup and archive tools.
- 20–30% of Microsoft 365 users leverage a third-party backup and protection tool/service.

WHAT'S IMPORTANT

- Growing reliance on SaaS application suites such as Microsoft 365 means organizations are responsible for ensuring data remains secure and accessible.
- Enterprises must understand their shared responsibility when it comes to data protection for SaaS applications.
- Organizations that know their role within the shared responsibility model will be better able to identify gaps and develop a comprehensive data protection strategy.

SaaS Backup and Data Protection: Market Context and Key Benefits

SaaS applications such as Microsoft 365 (and previous versions of Office 365) are considered fundamental for many enterprises looking to modernize their employee experience, introduce new means of collaboration, and create a digital workplace architecture. However, the native data protection and recovery capabilities offered by SaaS application suites often do not meet the specific needs of every organization. Many organizations have unique needs regarding data protection and retention due to industry or regulatory requirements.

The real danger is when organizations believe that native capabilities give them all the data protection they need for their specific use case or industry.

As a result, many enterprises adopt third-party solutions to augment their SaaS applications. When delivered as backup-as-a-service or disaster recovery-as-a-service solutions, these third-party services are considered by IDC to be part of the data protection-as-a-service (DPaaS) market. Demand for these services is significant: IDC forecasts the DPaaS market will grow at an 19% CAGR from 2021 to 2025, totaling $18.4 million, compared with just 2.7% CAGR for traditional data replication and protection software solutions over the same forecast period. This pace of growth of the DPaaS market is an important indicator of the demand for backup and disaster recovery for SaaS applications within enterprises.

Key Benefits: Why Organizations Need a Comprehensive SaaS Backup Strategy

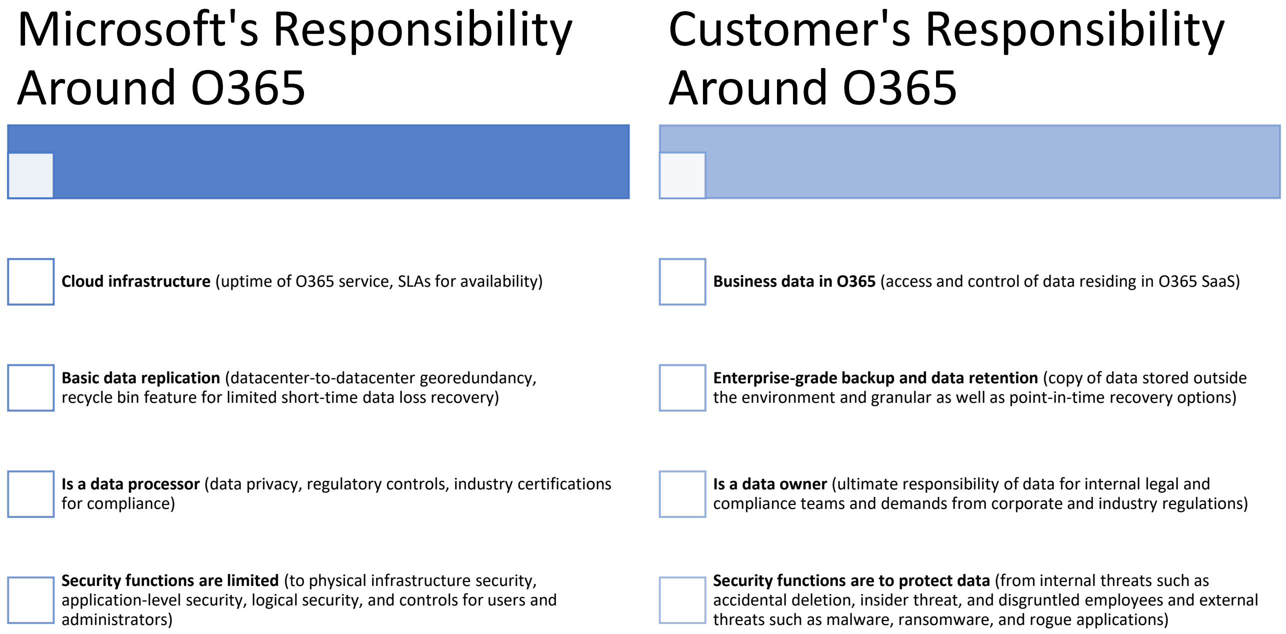
Simply put, as the use of SaaS productivity suites such as Microsoft 365 and Google Workspace grows, so do their data footprints. And as these footprints grow and amass increasingly sensitive and business-critical information, this data must remain available, secure, and compliant at all times. However, IDC research shows that data protection for Microsoft 365, in particular, is still an afterthought.

Surveys conducted by IDC over the past three years consistently indicate that 60–70% of Microsoft 365 users rely on the native/default backup and archive capabilities provided by the application. And on average, only 20–30% of Microsoft 365 users leverage a third-party backup and protection tool or service. IDC believes that native backup features and default retention in Microsoft 365 are good starting points, but they are typically not comprehensive enough for all compliance and business continuity needs. The real danger is when organizations believe that native capabilities give them all the data protection capabilities and tools they need for their specific use case or industry. In conversations with Microsoft 365 users, IDC observes that many users confuse Microsoft's availability service-level agreements (SLAs) with a comprehensive backup strategy, while others don't see the need to deploy a backup solution/strategy that is specific to cloud services and independent from their traditional backup solutions.

Organizations adopting cloud services and applications need to fully understand the "shared responsibility model."

Organizations adopting cloud services and applications need to fully understand the "shared responsibility model," which outlines the division of responsibility between a cloud provider (data processor) and cloud user (data controller), as illustrated in Figure 1. Understanding this breakdown of responsibility for data protection and compliance can help organizations identify where native capabilities may be lacking and where service additions/augmentation may be necessary to ensure comprehensive data protection for their given use case or application suite.

FIGURE 1: ***Microsoft 365 Vendor-Customer Shared Responsibility Model***



Microsoft's Responsibility Around O365

□ **Cloud infrastructure** (uptime of O365 service, SLAs for availability)

□ **Basic data replication** (datacenter-to-datacenter georedundancy, recycle bin feature for limited short-time data loss recovery)

□ **Is a data processor** (data privacy, regulatory controls, industry certifications for compliance)

□ **Security functions are limited** (to physical infrastructure security, application-level security, logical security, and controls for users and administrators)

Customer's Responsibility Around O365

□ **Business data in O365** (access and control of data residing in O365 SaaS)

□ **Enterprise-grade backup and data retention** (copy of data stored outside the environment and granular as well as point-in-time recovery options)

□ **Is a data owner** (ultimate responsibility of data for internal legal and compliance teams and demands from corporate and industry regulations)

□ **Security functions are to protect data** (from internal threats such as accidental deletion, insider threat, and disgruntled employees and external threats such as malware, ransomware, and rogue applications)

Source: IDC, 2021

Building the Business Case for SaaS Backup: Mitigate Ransomware Attack and Manage Data Growth

Historically, many businesses viewed data protection and backup solutions as overly expensive insurance policies. However, the growing criticality of SaaS application suites to modern digital businesses is quickly forcing a change in this perception. This shift in perception is also helped by the fact that modern backup and data protection solutions offer more than just backup for a specific application. They include tools for compliance, analytics, data management, and performance/cost optimization, which can help enterprises not only back up and recover their data but also implement more automated processes and comprehensive data management strategies.

For this analysis, we focus on two key trends that we believe can help modern digital businesses build their business case for the need for SaaS backup and data protection tools. The trends can be broadly categorized as the growing threat of ransomware attacks and cost-effective management of exponential data growth. Each trend is explored in depth in the following sections.

Mitigate Ransomware Attacks

Malware, and specifically ransomware, is one of the highest concerns of business and IT leaders alike, according to a number of IDC data protection surveys. IDC research shows that only 13% of enterprises that reported experiencing a ransomware attack *did not* pay the ransom. Furthermore, the average ransom amount paid was almost $250,000. Ransomware attacks don't just happen to "the other guy." Attacks happen to nearly every organization. While the majority of attacks are unsuccessful, one well-executed attack can be devastating to an organization both economically and reputationally. Although most people think ransomware is performed by external attackers, the possibility of insider threats should not be underestimated.

The threat of ransomware has become so impactful to many organizations that they are integrating ransomware response and recovery as a component of their backup and disaster recovery strategies. In the past, organizations could take a risk and avoid disaster recovery deployments because they were not in a zone prone to natural disaster; this is not the case with ransomware. Today, any organization attached to the internet is in a ransomware "zone" and at risk of a potential attack. Further, many ransomware attacks are successful and profitable because organizations do not have adequate data recovery capabilities in place. We have identified four key reasons why data recoveries often fail when organizations are faced with responding to a ransomware attack:

- **Lax defense.** Cyberintrusion detection is a constant effort and evolution. Artificial intelligence (AI) systems are becoming indispensable in detecting evolving risk. Organizations that are not sufficiently vigilant or that do not invest appropriately can quickly become vulnerable.
- **Inadequate preparation.** Cyber-recovery is a combination of people, process, and technology. Technology alone is not enough; processes to avoid insider threats and practiced response teams are needed to recover quickly.
- **Inadequate immutability.** Some immutability schemes can be circumvented by simply adjusting storage policies or changing system dates outside the immutability time frame.
- **Compromised air gaps.** Air gap schemes that open data and control paths at the same time create the possibility of air-gapped copies becoming corrupted, especially by insiders.

Many organizations are accelerating their deployment of backup and disaster recovery solutions in the cloud to respond to ransomware. There is plenty of room for solution differentiation based on data type, workload platform, "DIY" to "white glove," recovery orchestration, and many other factors. An additional premium is being placed on data protection solutions that incorporate AI or machine learning (ML) to help the system adapt dynamically to evolving ransomware and malware threats and ensure that backup copies do not also become infected with malware or ransomware.

Manage Enterprise Data Growth

Data growth continues within all modern organizations, and all enterprises should be considering a data protection strategy that addresses backup and data management needs for multiple workload types and locations (e.g., on premises, cloud, edge) — one that puts an emphasis on flexibility and scalability to accommodate enterprises' insatiable appetite for data. According to IDC, the enterprise storage systems install base in aggregate (inclusive of stored data in public cloud, dedicated and private cloud, and traditional IT environments) will grow at a five-year CAGR of 30.9% — reaching 5,451 exabytes in 2025. This data growth puts many organizations in a precarious position where they are forced to manage and protect growing volumes of data without adequate budgets. It is rare to find IT budget growth in line with data growth. In many cases, this mismatch between IT budgets and data growth results in a lack of adequate tools for data management and protection as capacity expansion takes precedence in the short term.

This potential trade-off is one of the reasons why data growth is insidious to traditional data management and protection — it is a creeping problem that becomes worse over time if it is left unaddressed and unmanaged. Infrastructure sized for today's data volumes gradually becomes insufficient, often to be discovered when SLAs (especially recovery SLAs) are missed. Traditional backup methodologies can no longer cope with such data volumes. There are new data types, protocols, containerization methods, and changing data protection requirements. As a result, enterprises are increasingly turning to data protection service providers to manage growing volumes of data, and the associated need for data management and protection, within a single environment. These data protection platforms and services can be provisioned to allow data to be gathered from and protected across a wide variety of repositories and/or applications. In addition, the service delivery aspect of these solutions ensures that the underlying infrastructure and associated data management and protection tools are continuously up to date.

Considering Afi

Afi is a cloud-to-cloud SaaS backup provider focused on Office 365 and Google Workspace data protection. Released in 2016, Afi provides services for midsize to large enterprises (typically with 5,000+ users). Afi currently protects over 10,000 Google Workspace and O365 domains, which equates to over 20 petabytes of data under protection. The vendor built its business on SaaS data protection but is expanding into public cloud infrastructure (IaaS) and Kubernetes backup. The following offerings are part of Afi's service portfolio:

- **Afi Google Workspace (G Suite) Backup:** Provides point-in-time restoration of G Suite data using high-frequency snapshots; includes user self-service capabilities, automated backup schedules, automated G Suite user updates, granular access controls for administrators, and audit capabilities; leverages Afi's intelligent ransomware protection capabilities
- **Afi Microsoft (O365) Backup:** Microsoft 365 backup including full support for Teams, SharePoint, and OneDrive; point-in-time recovery and integration with Azure AD; automatic management of Microsoft 365 user groups, along with granular access control and auditing for administrators, with the ability to enable self-service for end users to recover their data; leverages Afi's intelligent ransomware protection
- **Afi Kubernetes Infrastructure Backup:** Deployed to protect persistent storage associated with distributed Kubernetes applications; provides a single solution to manage and protect all major cloud Kubernetes distributions (e.g., EKS, GKE, AKS, Tanzu); allows restoration of an entire application or only some of its components to the same cluster or a different cluster with automatic reconfiguration; uses incremental replication and provides command-line interface access as well as API access for integration with a broad range of infrastructure management and DevOps tools and platforms

Afi Core Capabilities and Key Differentiators

Afi is a cloud-native backup provider. In this case, cloud native means that Afi's service is built on a distributed Kubernetes application architecture that runs on the public cloud (GCP and AWS specifically). This architecture gives Afi a massive amount of scalability in terms of resources (compute and storage) as well as a global infrastructure footprint, and it makes scalability one of Afi's key differentiators from an infrastructure perspective. The vendor has designed its Microsoft 365 and Google Workspace data protection platforms to accommodate deployments with over 100,000 seats (users) without any degradation in service levels or performance.

Afi offers a range of enterprise data services in addition to its core suite of continuous backup and data protection services. This includes data encryption (with a BYOK option), data tiering, granular data retention and archival settings, automatic metadata creation and labeling of backups, automated data protection management at scale using AAD/Google OU structure, role-based access and permissions for administrators and end users, data residency management to enable compliance with regional data privacy regulations, reporting and management APIs, and integrations with major cloud IAM providers.

With regard to ransomware protection, Afi has invested heavily to develop its own internal solutions, which are integrated into all its services. Afi's anti-ransomware is powered by AI and designed to aid enterprises in the detection and mitigation of and effective response to ransomware. Afi has developed an AI engine — in this case a neural network — that is trained to identify and flag potential malicious behavior by analyzing patterns in backup data ingestion/access as well as individual user behavior. This AI engine is augmented with the collection of third-party security and outage data, including vulnerability feeds and known ransomware activity reports, as well as downtime feeds from leading cloud service providers (e.g., AWS, Azure, GCP). The engine helps Afi deliver a highly differentiated level of proactive data protection and security.

Simplicity is another key tenet of Afi's business and platform. Service pricing is designed for simplicity with a user-based licensing scheme and limited fee structure. Enterprises can license Afi the same way they pay for their Microsoft 365 service ($/user/month). Furthermore, enterprises can license all their SaaS users or a subset depending on their needs. Simplicity is also reflected in the design of the service itself. Administrators manage all backup data, policies, roles, and self-service needs within a single, web-based UI and console.

Challenges

- Afi is relatively new to the SaaS backup market compared with some competitors that have existed in the space for 10+ years. Any emerging market entrant such as Afi needs to establish its brand recognition and perception as well as trust to achieve success among midsize to large enterprises. IT buyers in this segment of the market tend to rely on trusted brands to secure and back up critical data. Afi is addressing this challenge by developing an increasingly robust portfolio of customers, partners, and case studies.

- Afi is competing in an increasingly crowded market. The continued adoption of SaaS applications and IaaS resources within enterprises has led almost all major data protection providers to develop solutions (either organically or through acquisition) for both SaaS data protection and protection for virtual machines (VMs) and storage deployed on leading cloud IaaS environments such as AWS, Azure, and GCP. Providers in this market will face growing pressure to prove their differentiation and win market share by providing more advanced product capabilities as well as better support and customer service at increasingly lower price levels.

Conclusion

By not extending data protection to SaaS environments such as Microsoft 365 or Google Workspace, enterprises are exposing their application data to compliance issues, data loss, security vulnerabilities, ransomware attacks, and business continuity risks. Backup for fast-growing SaaS environments such as Microsoft 365 is no longer an option or a "nice-to-have" — it should be considered mandatory for adequate data security, control, and protection. Most data protection vendors offering backup and recovery for SaaS environments are continuously adding more tools and services to their portfolios.

IDC recommends that organizations evaluating or purchasing a backup solution ensure that the solution they choose offers flexible pricing and deployment, seamless integration to the SaaS application environment, enterprise-grade backup features, coverage of multiple SaaS environments, and the ability to scale to a massive user base without any service degradation.

About the Analysts

Andrew Smith, *Research Manager*

Andrew Smith is a Research Manager within IDC's Enterprise Infrastructure Practice. Andrew's research focuses on public cloud infrastructure-as-a-service platforms and solutions, with specific focus on storage services. Andrew contributes to market sizing and forecast efforts across IDC's public cloud IaaS segments, as well as adjacent markets like multicloud data management, data protection as a service, and public cloud cold storage.

Archana Venkatraman, *Associate Research Director*

Archana's primary research coverage is cloud data management. She covers multiple topics including data protection, edge-to-cloud data trends, application and data availability, compliance, data integration, intelligent data management, DataOps, data quality, and multicloud priorities and trends. Archana is also a co-lead of the cloud practice and an active contributor to IDC's Europe's DevOps and AI research practices.

MESSAGE FROM THE SPONSOR

Afi provides reliable and highly scalable backup service with full-fidelity support of cloud data sources. Our cloud-native platform is based on container architecture and delivers secure data protection with encryption in-transit and at rest, customer-managed encryption (BYOK) capabilities, extended audit, alerting, Azure AD/Okta integration, and multiple unique features including AI-assisted recovery and anti-ransomware protection. Afi is used by thousands of customers from small- and medium- sized businesses to large enterprises with more than 100,000 employees and strict security requirements.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.