451 Research
Pathfinder Paper

November 2024

Buyers' guide: Microsoft 365 data protection

Commissioned by

veeam

S&P Global
Market Intelligence

Table of contents

Executive summary

Microsoft 365 underpins key workloads for most organizations, and the high cost of outages and data loss have dramatically increased the importance of data protection tools such as backup.

The software-as-a-service (SaaS) delivery of Microsoft 365 introduces particular considerations and challenges that organizations must keep in mind as they evaluate data protection offerings. This buyer's guide discusses key capabilities for customers to consider when evaluating backup offerings, and looks at how evolution of the SaaS market could influence hybrid and multicloud infrastructure decisions in the near future.

Key findings

- **Outages are becoming more costly.** The mean cost of outages has risen steadily from $1.56 million in 2022 to $2.33 million in this most recent study. About 47% of outages cost more than $1 million, up from 36% in the 2023 iteration of this study. Outages lead to numerous consequences, including lost worker productivity, data loss, lost revenue and lost customer loyalty. Security incidents including ransomware have been a top cause of outages.
- **Protection of SaaS data continues to evolve.** One-third (33%) of respondents use third-party cloud-to-cloud data protection for their SaaS data, while 32% rely on their cloud vendor for data protection. Respondents most commonly cite Microsoft 365 (67%) as a SaaS platform in need of backup protection, followed by Google Workspace (46%) and Salesforce (40%). Only 5% of respondents say they are not backing up their SaaS applications, which marks an incremental improvement from 6% in 2023 and 9% in 2022.

Data protection for SaaS is a growing concern

The frequency and cost of outages is driving organizations to enhance their data protection and resiliency. Data protection for SaaS workloads has become a top concern because platforms such as Microsoft 365, Salesforce and Google Workspace support essential production workloads for most organizations.

Current trends have made data protection for SaaS essential for all organizations, regardless of size.

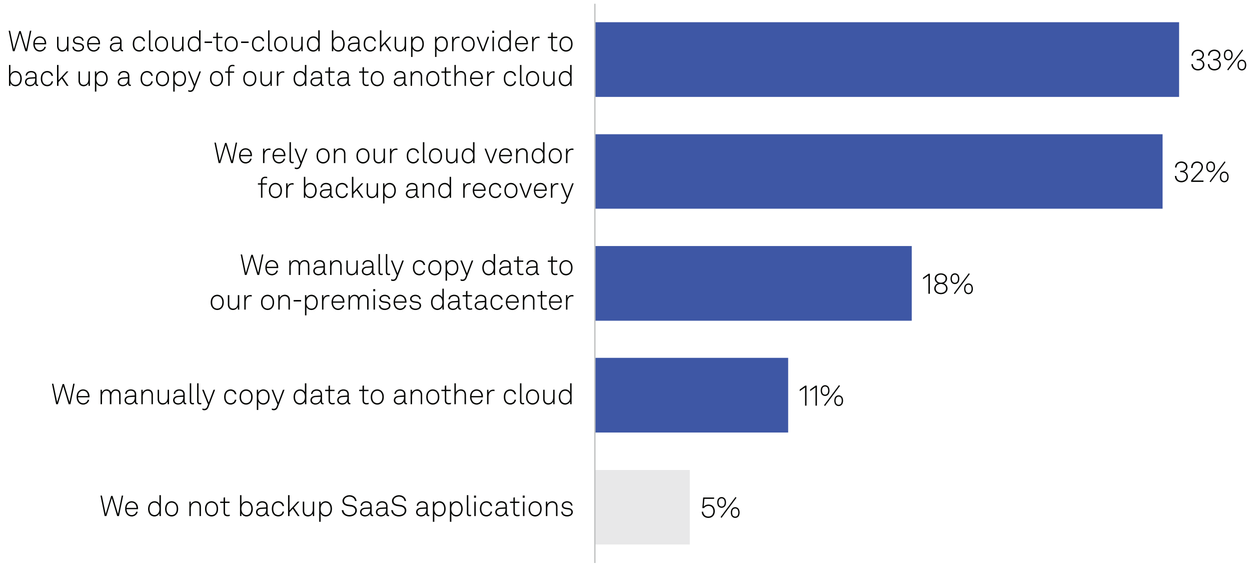
Outages are common and costly: Most organizations have experienced a significant outage that led to data loss or loss of employee productivity. Two-thirds (67%) of respondents have experienced an outage at some point, and more than 30% have experienced one in the past two years. Respondents say their outage costs have grown substantially from an average of $1.56 million in 2022 to $2.33 million in 2024, representing a 49% increase in the past two years. Nearly half of recent outages (47%) cost more than $1 million, up from 36% in 2023.

SaaS service failures and security incidents are top causes for outages: SaaS and public cloud service failures caused a quarter of recent outages among survey respondents, which highlights the need for resiliency enhancements. While a third-party backup cannot fix issues at the SaaS provider level, local backup could allow staff to locate and access important data while the SaaS cloud is unavailable. Security issues such as ransomware (28%) are another top cause of outages. Data and workloads running in SaaS may be deleted, altered or encrypted by a ransomware attack or other security incident if SaaS login credentials are stolen.

Organizations are seeking third-party tools for data protection for SaaS: Just 5% of respondents say they are not protecting SaaS workloads and data. A third of organizations are already using third-party data protection tools to facilitate cloud-to-cloud backups, while a similar number are using native backup tools from their SaaS provider (see Figure 1). Nearly a third (29%) are manually copying data to another cloud or an on-premises datacenter, which is slightly better than having no protection but could lead to a false sense of security. Manual copy operations are prone to error, especially if the homegrown tools and scripts are not maintained properly or if the staffers writing the scripts and tools leave the organization without documenting their work.

Third-party SaaS data protection is on the rise

Figure 1: SaaS customers are relying on third-party backup providers



Q. What is your organization's primary data protection strategy for SaaS applications (e.g., Salesforce, Microsoft 365, Google Workspace [formerly G Suite], etc.)?
Base: All respondents (n=427).
Source: Voice of the Enterprise: Storage, Disaster Recovery 2024.

Shared responsibility

Before deciding on a data protection offering for Microsoft 365, organizations should consider the allocation of shared responsibility between a customer and the vendor or service provider.

Organizations that want to assume the bulk of shared responsibility would likely lean toward purchasing and implementing an on-premises deployment using hardware and software they purchase and maintain. The organization's responsibility in this case would also include creating data protection policies, backup scheduling, backup validation testing, provisioning and end-user support.

In contrast, organizations that want to outsource as much of the shared responsibility burden as possible would likely choose a managed backup-as-a-service (BaaS) deployment in which the service provider handles implementation, provisioning and life-cycle management for the servers, storage system and cloud storage services consumed. A managed BaaS provider would also assume day-to-day operational burdens associated with provisioning, validating and customer support for the data protection implementation. The customer would monitor the usage of the managed BaaS and plan for updates.

Three different ways to implement

Broadly speaking, there are three ways to protect Microsoft 365, and each method provides different levels of protection, assistance and data control to match an organization's needs.

Backup software

For companies that have experience running on-premises data protection, a backup software package deployed in-house may be the most seamless option. Organizations with experience running legacy backup infrastructure would have a flatter learning curve for deploying, maintaining and optimizing in-house data protection. With their methodologies and policies in place, the need to train staff is lessened, and these organizations may use existing storage assets to consolidate backup data and avoid extra hardware purchases.

Backup service

Backup services allow customers to quickly protect their Microsoft 365 accounts and would likely appeal to organizations that lack the existing infrastructure, processes and experienced staff to run data protection services in-house. With backup services, customers may attain lower overall costs through bundled solutions that have key capabilities such as unlimited backup storage.

Service providers and backup vendors currently provide backup services, and they typically provide various service levels that allow customers to tailor their deployments based on the requirements of the Microsoft 365 accounts they are protecting. Add-on services for premium features such as accelerated ransomware recovery are typically available for additional protection when desired.

With backup services, backup data is typically stored in the service provider's cloud storage environment, which may not be suitable for all types of customers, depending on regulatory and data sovereignty requirements, among other factors.

Managed BaaS

In a managed backup-as-a-service (BaaS) deployment, a service provider provisions and manages the data protection infrastructure, including backup servers and related backup storage. Backup data may be housed in any combination of on-premises storage infrastructure, the service provider's cloud storage service, or a public or private cloud environment. Managed service providers (MSPs) provide expertise and guidance for organizations seeking to offload management and operational responsibility for data protection services. Among the three deployment options, managed BaaS offloads the greatest degree of responsibility for data protection, but it is also likely to entail higher total costs and a longer commitment compared with a backup service.

Because managed BaaS can be deployed in a customer's datacenter or leased colocation environment, these solutions are attractive for organizations in compliance-sensitive verticals such as financial institutions and healthcare, which may not be willing or able to store their data in a public cloud or with a backup service provider.

What to look for

Though the data protection space has many mature and innovative offerings, choosing the wrong platform could put an organization's data and business at risk and lead to higher costs. Common data protection best practices should be factored into the evaluation of any solution. An example is the 3-2-1 rule, which calls for organizations to store three copies of data (including the original), with backups stored on two different types of media, and with one copy stored off-site. The rise of security threats such as ransomware and the ongoing evolution of compliance requirements are also major factors that highlight the need for immutable storage and advanced data management to control where and how data is stored and accessed.

When choosing how to protect your organization's Microsoft 365 implementation, these are key capabilities to keep in mind:

Backup customization

Microsoft 365 data protection solutions may provide a variety of customization options to suit company-specific requirements.

- **Backup location:** When choosing a backup service provider, organizations will likely need to check the geographic storage options available to ensure organizational data is stored in the most appropriate region. Some organizations have strict data sovereignty and compliance requirements that may prevent them from storing data in specific countries.
- **Flexible backup selection:** The business value and criticality of data and end-user accounts varies dramatically within an organization, and it may not be necessary to back up every account and workload. A flexible backup solution does not force the customer to back up the entire organization, but allows the customer to choose individual Microsoft 365 users, groups, SharePoint sites and Teams for backup.
- **Flexible scheduling:** Flexible backup solutions allow configuration of data protection to match stakeholder requirements. For example, important accounts may be set to run backups every few minutes, while accounts with less stringent requirements may be set for daily or weekly increments. Some offerings will have configurable recovery point objective (RPO) settings to match the organization's service-level agreements (SLAs) and limit the data that could be lost after an incident.
- **Customizable retention:** Flexible solutions offer the ability to customize the retention period for backups. In some cases, such as in highly regulated environments, data may need to be retained in perpetuity. In other cases, such as in certain financial and legal contexts, an organization may want to ensure that backups are deleted as soon as data is no longer required.
- **Immutable storage management:** Another key element, especially with the rise of ransomware, is a backup platform's ability to manage immutable storage to preserve backups and protect them from intentional and unintentional deletion or encryption. For organizations looking to store their backups in a public cloud storage service, the backup platform must support interoperability to manage retention lengths. Security features such as multi-factor authentication should also be available to ensure an intruder cannot easily disable immutability and delete backups.

Recovery criteria

Backups are ineffective without recovery operations. Organizations should keep certain factors in mind when evaluating recovery capabilities:

- **Flexible data restoration options:** An effective backup offering must provide recovery options that match stakeholders' requirements. In some cases, a granular data restore operation that allows a client to restore a specific file, folder or email message may be required in the event of an accidental deletion or file corruption. In contrast, to quickly recover from a large-scale incident such as a ransomware attack, a bulk restoration may be required to restore data for multiple users or even the entire organization.
- **Restore location flexibility:** In some cases, it may be desirable to restore data to an alternate location. For example, if a terminated employee deleted messages and files prior to departing, the company may want to restore that data to a manager's or compliance officer's inbox or to a file share.
- **Deep application support:** The depth of support for applications varies among backup offerings. Organizations will likely want a solution that protects all aspects of an application. For example, with Teams, an advanced backup platform would not only protect the data within the application, but also Teams channels, posts and tabs, team memberships and other relevant settings. Incomplete restorations can lead to lost data and could force end users to waste valuable time reconfiguring applications to their preferred settings.
- **Advanced search:** The ability to locate data is essential for restoration operations. When evaluating a backup platform's search capabilities, organizations will want to note how well the search interface can combine multiple criteria to narrow down datasets to focus on the specific data that needs to be restored.
- **Self-service restoration:** Most employees and virtually all knowledge workers depend on Microsoft 365 daily. Self-service recovery portals allow clients to initiate the retrieval process without requiring human intervention. This capability can dramatically reduce the operational burden and the number of request tickets sent to a helpdesk for data restoration. Self-service restoration can also help workers recover data faster and may be done after hours when fewer IT staff members are available.

Services and support

The level and quality of technical support should also be a factor when evaluating Microsoft 365 data protection options. Vendors typically provide different levels of support at various price points. Organizations should evaluate a prospective vendor's technical support capabilities during the trial period, which may last up to 60 days. For organizations with more lenient requirements, a standard technical support contract that allows for updates and calls during business hours may be sufficient. For those with higher resiliency requirements, premium support may provide 24/7 access to support personnel and could also include SLA guarantees to ensure the fastest response times.

Future considerations

An organization's data protection requirements for Microsoft 365 may change as compliance and business requirements evolve. To ensure that data protection is future-proofed, the following elements should be considered:

Relationship with SaaS provider

Organizations would be wise to seek out Microsoft 365 data protection vendors and service providers that have a strong relationship with Microsoft and the product team. A strong data protection vendor would have integration with the SaaS vendor's API and would have a product development cycle committed to adding new features and updating the platform to leverage new APIs and protect new workloads and applications as Microsoft 365 expands and evolves.

Microsoft 365 Backup Storage is a key service that Microsoft created to support third-party backup applications, and data protection platforms should have the ability to support it. Given that Microsoft 365 Backup Storage resides in Microsoft's cloud infrastructure, the service can provide high-speed recovery at local recovery speeds, which is essential for meeting recovery time objectives (RTOs) to get the client up and running quickly after an incident.

The rapid development and growing importance of Microsoft's AI functionality is another key area, and data protection vendors should have programs to work with Microsoft Copilot and to integrate with and protect future AI services.

Broad platform coverage

To simplify data protection across all relevant workloads, customers will likely want to choose a data protection platform that can protect virtual machines, physical servers, storage systems (i.e., network-attached storage) and other key assets and services such as Microsoft Entra ID. With the growing importance of cloud-native workloads, organizations will likely benefit from platforms that are designed for Kubernetes and can take advantage of the scalability of this architecture.

Beyond Microsoft 365, organizations are looking to protect additional SaaS platforms such as Salesforce, Google Workspace and ServiceNow. As new SaaS platforms emerge, data protection vendors should have expansion roadmaps to add protection for these applications as they grow in importance.

Avoid vendor lock-in

Customers would be wise to avoid data protection offerings that require them to deploy and maintain proprietary hardware and software. While a solution with end-to-end hardware and software integration could have ease-of-use benefits, dependency on a single vendor for hardware and software creates lock-in that would make it harder to shift to a different offering in the future.

For example, on the hardware side, it is common for customers to get competitive bids from storage vendors to reduce costs. A fully integrated solution would sacrifice this leverage and could lead to higher spending over the lifetime of the deployment. To match the ease of deployment and simplicity of an integrated or bundled offering, organizations may seek out vendors and service providers with comprehensive support programs that will continue to deliver at a high level, even if a hardware or software component is changed or added.

Vendor lock-in is also an issue when evaluating service providers and cloud storage services. Organizations should consider working with a vendor that does not charge harsh penalties for leaving. Customers would also likely benefit from working with a vendor that allows easy movement from one deployment model to another, such as a transition from on-premises software to BaaS. Vendors that allow customers to switch from one cloud storage service to another as needed can help organizations to prevent long-term vendor lock-in.

About the author

Henry Baltazar

Research Director, Storage

Henry Baltazar is research director of the 451 Research Storage channel within S&P Global Market Intelligence, with a focus on data storage. In his current role, Henry analyzes the market trends around environmental, social and governance (ESG) storage challenges, infrastructure modernization and resiliency. He publishes reports on trends in data storage, disaster recovery and hybrid cloud. He is often cited as a subject expert by publications such as MIT Technology Review, Forbes and TechTarget.

Henry arrived at S&P Global Market Intelligence through its 2019 acquisition of 451 Research, where he began working as an analyst in August 2006. After spending three years running the storage research practice at Forrester, he returned to 451 Research in 2015 to fill the research director role and lead the storage practice. Henry graduated from the University of California, Berkeley with a bachelor's degree in environmental sciences.

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About S&P Global Market Intelligence

At S&P Global Market Intelligence, we understand the importance of accurate, deep and insightful information. Our team of experts delivers unrivaled insights and leading data and technology solutions, partnering with customers to expand their perspective, operate with confidence, and make decisions with conviction.

S&P Global Market Intelligence is a division of S&P Global (NYSE: SPGI). S&P Global is the world's foremost provider of credit ratings, benchmarks, analytics and workflow solutions in the global capital, commodity and automotive markets. With every one of our offerings, we help many of the world's leading organizations navigate the economic landscape so they can plan for tomorrow, today. For more information, visit www.spglobal.com/marketintelligence.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia-Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global keeps certain activities of its divisions separate from each other to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain nonpublic information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.