 Business Impact Brief

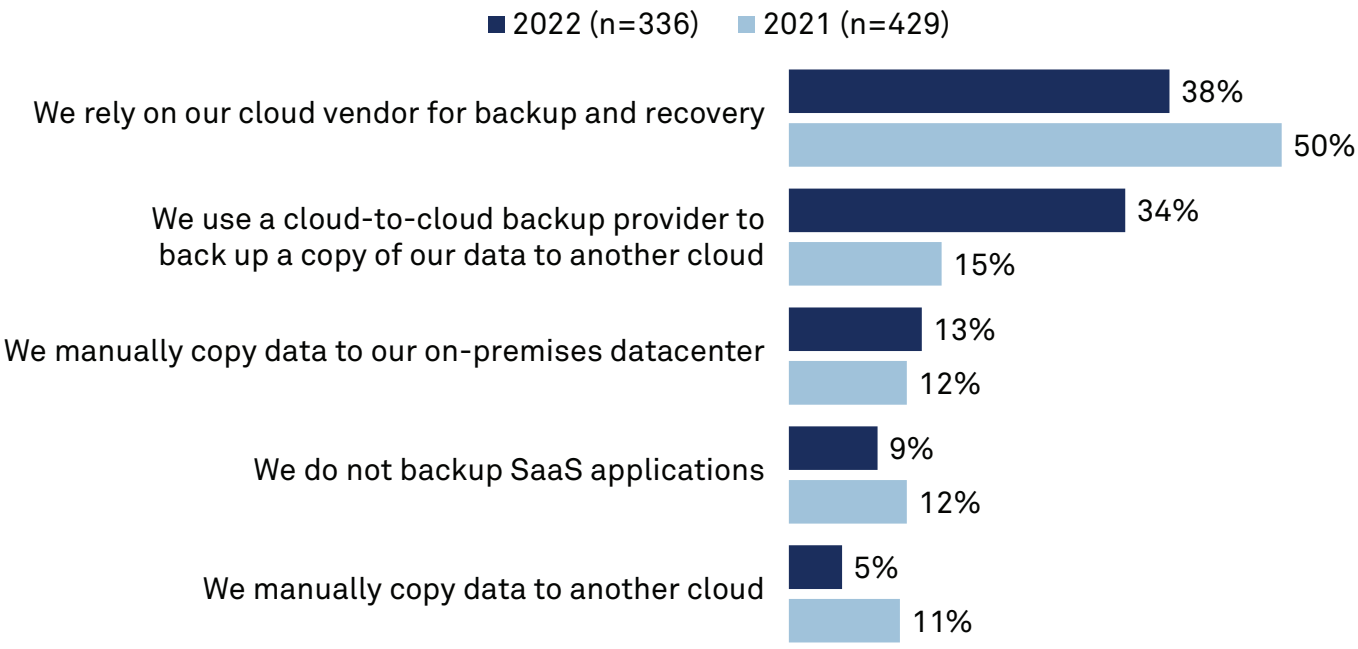
Rise of Microsoft 365 Creates Data Protection Issues

The 451 Take

A hybrid IT environment, which leverages on-premises and cloud services resources interchangeably, is the desired state for many organizations. But as these customers ramp up their use of public cloud and SaaS services and applications, they must implement a consistent and comprehensive data protection strategy across all these environments. There remains a major gap in the data protection coverage of SaaS platforms such as Microsoft 365 (M365), Salesforce and Google Workspace. In the Voice of the Enterprise: Storage, Data Management & Disaster Recovery 2022 study, 43% of respondents said they are considering purchasing a backup service to protect their M365 data, well ahead of other SaaS platforms such as Microsoft Dynamics (21%), Google Workspace (14%), Salesforce (13%), ServiceNow (4%) and Dropbox (2%). This suggests that M365 is a key platform requiring enhanced data protection.

In the study, 38% of organizations said they still rely solely on their cloud and SaaS vendors for backup and recovery (see Figure 1), down from 50% in the previous year's study. Meanwhile, 34% of respondents said they are using a cloud-to-cloud backup provider to protect their SaaS data, up significantly from just 15% a year ago. Despite this market momentum, 9% of respondents still do not back up their SaaS applications, and 13% of respondents manually copy SaaS data to their on-premises datacenters, an approach that lacks the automation, reporting and consistency checking that third-party backup tools provide.

Data Protection for M365 and Other SaaS Platforms Is Evolving



Q: What is your organization's primary data protection strategy for SaaS applications (e.g., Salesforce, Office 365, Google Workspace (formerly G Suite), etc.)?

Base: All respondents

Source: 451 Research's Voice of the Enterprise: Storage, Data Management & Disaster Recovery 2022 and 2021

Business Impact

Accelerated recovery expectations are rising. M365 customers have a low tolerance for downtime and data loss since a significant outage prevents them from being productive and hampers collaboration between employees, as well as with business partners and customers. Recovery time objectives have become so stringent that even daily backups cannot provide adequate protection for most clients, which are not willing to lose hours of productivity to an outage. To meet these needs, organizations should seek out backup services with powerful search and granular recovery capabilities. This will allow them to quickly find the data to recover and restore jobs as small as individual email message recovery all the way up to restoration operations for entire SharePoint sites.

Data archive can drive SaaS cost reduction. M365's native data protection tools, which include versioning and post-deletion file retention, are limited to an approximately 90-day retention window, beyond which accidentally deleted or corrupted files cannot be recovered. While customers could upgrade to Compliance Center retention policies to achieve unlimited retention, these services cost more per user per month, which can lead to a bloated monthly SaaS bill. By using a backup service with intelligent archiving capabilities, organizations can move older and infrequently accessed data copies to a less expensive cloud storage repository that can retain data even if they decide to shut down their M365 accounts.

Ransomware threat amplifies the need for immutable storage. Backup repositories serve as the safety net for organizations in the event of a disaster, which is why bad actors are now looking to attack them to prevent customers from restoring their data and operations after a successful attack and increase the pressure on customers to pay the ransom. Using immutable storage and air-gapped storage options, organizations can prevent attackers from compromising and deleting backup copies, even if bad actors compromise the primary systems or cloud accounts.

Compliance visibility and reporting is an area of need. The majority of organizations have data retention and data deletion policies that determine their long-term data management. To ensure that they are meeting compliance guidelines, employees responsible for compliance need to spend large amounts of time documenting and validating the health of their data repositories. Intelligent data protection tools can provide reporting to reduce the compliance burden while keeping the organization audit-ready in the event of a compliance inspection or e-discovery request.

Looking Ahead

An organization's unique and proprietary data is often its most valuable asset, and M365 is a platform where extremely valuable documents, messages and other content are created, shared and stored. As such, comprehensive data protection for M365 is a key requirement not only to preserve data, but also to make sure operations can be restored in a timely manner should a cyberattack, disaster or significant outage occur.

Steps taken to enhance data protection for M365 and other SaaS platforms can provide substantial benefits beyond basic data protection. Intelligent tools that can locate, identify and analyze data usage patterns can help the members of an organization quickly locate and access critical data when they need it. For compliance-sensitive organizations such as financial services, healthcare and government agencies with strict data management and auditing requirements, data protection tools could provide the reporting to respond to audits. Automated data archiving capabilities can also provide cost savings for organizations by moving data to less expensive mediums and eliminating the need for expensive premium services that could potentially lock in customers to a SaaS platform.