451 Research® | PATHFINDER REPORT

Taking Control of Your Office 365 Data

COMMISSIONED BY

VEEAM

MARCH 2019

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 THE AUTHOR

STEVEN HILL

SENIOR ANALYST, STORAGE

Steven Hill is a Senior Analyst of Storage technologies. He covers the latest generation of hyperconverged systems, cloud-based storage and business continuity/disaster recovery solutions for enterprise customers.

Executive Summary

Modern software-as-a-Service (SaaS) applications such as Microsoft Office 365 can offer several advantages over the traditional software consumption model for many business customers, but the increased flexibility of the cloud-based licensing and the availability of shared cloud storage create a new set of challenges when it comes to data management. Application availability in the cloud is proving to be extremely resilient, but protecting Office 365 SaaS data from risks such as accidental deletion, security threats and retention policy gaps – as well as meeting the evolving security requirements of compliance-led data governance – dictates a continuing need for the traditional protection and control offered by automated and verifiable Office 365 backups.

SaaS vendors focus primarily on protecting their own infrastructure to meet their contractual service level agreements (SLAs), but that protection doesn't extend to customer data created and stored on those platforms. This is understandable when you consider the potential liability issues, and most SaaS licensing includes a clause that specifies data protection is the responsibility of the customer, not the SaaS vendor. This poses the potentially million-dollar question: 'What should you be doing to protect and control your Office 365 data?'

Key Findings

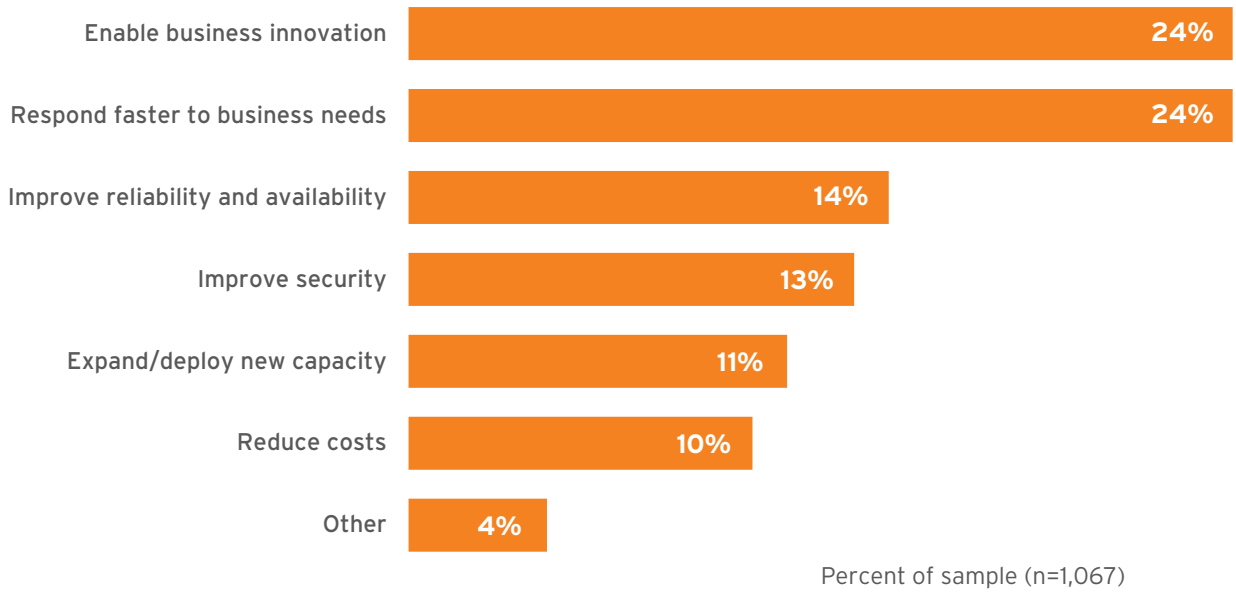
- **Office 365 email and documents shared and stored in SharePoint, OneDrive and Teams are the new business-critical data.** Many business continuity/disaster recovery (BC/DR) plans start with protecting key databases and other mission-critical applications, but the unstructured data generated by SaaS-based products is starting to grow faster than traditional database information and can have just as critical of an impact when lost or destroyed.
- **There is a common misconception that SaaS data in the cloud is inherently safe.** The public cloud is proving to be extremely reliable, and though SaaS-based platforms themselves are internally protected against service interruptions, it is the customer's responsibility to secure, protect and establish retention policies for this cloud-based data.
- **Expanded recovery and governance options are becoming nearly as important as the data backup itself.** Much of the value proposition of a backup platform for Office-type data lies in the flexibility of its recovery and management capabilities. While Office 365's SharePoint and OneDrive storage offers tools for data archiving and setting up workflows, this is not a replacement for an Office 365 backup where all data is independent of the cloud platform itself and managed based on a set of tools that offer more granular recovery, security and governance.
- **Data protection will be increasingly driven by new legal and compliance-based challenges.** Traditional data backup is specifically focused on preventing data loss, but e-discovery and privacy-based laws such as the EU's General Data Protection Regulation (GDPR) and the recent California Consumer Privacy Act of 2018 set new ground rules for data protection and governance. Maintaining an Office 365 backup can address many of the key requirements for data protection and security and can also serve as a reference dataset that can be analyzed to satisfy compliance-based rules that expect companies to be able to locate, disclose and even provide verifiable deletion of any data containing personally identifiable information on demand.

The Evolution of Business IT and the New Role of SaaS Data

In today's IT-driven business environment, speed is everything. This has been the case for decades, and the adoption of the right technology has been proven to be a major factor in the success and growth of companies in nearly every vertical market. Today, the cloud delivery model offers a flexible new way for businesses to consume applications, infrastructure, services and data, but the real challenge for IT still lies in finding the right combination of technology to meet business goals. To get an industry-wide idea of what those goals look like, we regularly ask more than 1,000 enterprise IT personnel – through our 451 Research Voice of the Enterprise (VotE) service – to weigh in on what's most important in their environments (Figure 1), and we consistently find that innovation and responsiveness rank as the top considerations.

Figure 1: Most important goals for enterprise IT over the next year

Source: 451 Research's Voice of the Enterprise: Digital Pulse, Vendor Evaluations 2018
Q. What is the most important goal for your organization's IT over the next 12 months?



Software as a service is one of the key technologies enabled by the cloud that helps to advance innovation and responsiveness. The SaaS model offers key features such as flexible licensing and version consistency that can help make end users more productive and interactive. From a business perspective, it's difficult to deny the convenience of the SaaS model, especially when it comes to suites of applications such as Office 365, which adds cloud-based collaboration capabilities to the task of creating and managing business-critical documents, email and other content.

In addition, Office 365 offers integrated public cloud storage options in the form of SharePoint, OneDrive and Teams that can reduce the need for on-premises storage and simplify shared data access for collaboration. But there's a common misconception that SaaS-based customer data is secure and protected because it's already 'in the cloud.' The simple fact is that it's not, and in the case Office 365, the licensing agreement clearly states that adequate data protection remains the responsibility of the customer. This is where business IT has to step in and help key stakeholders determine the appropriate data protection, security, availability and retention policies for their data, and then match that to the right combination of technology. While this may add some complexity to SaaS adoption at the front end, a coherent, hybrid data protection plan will more than pay for itself in the event of a systems outage that can impact business-critical or compliance-governed data.

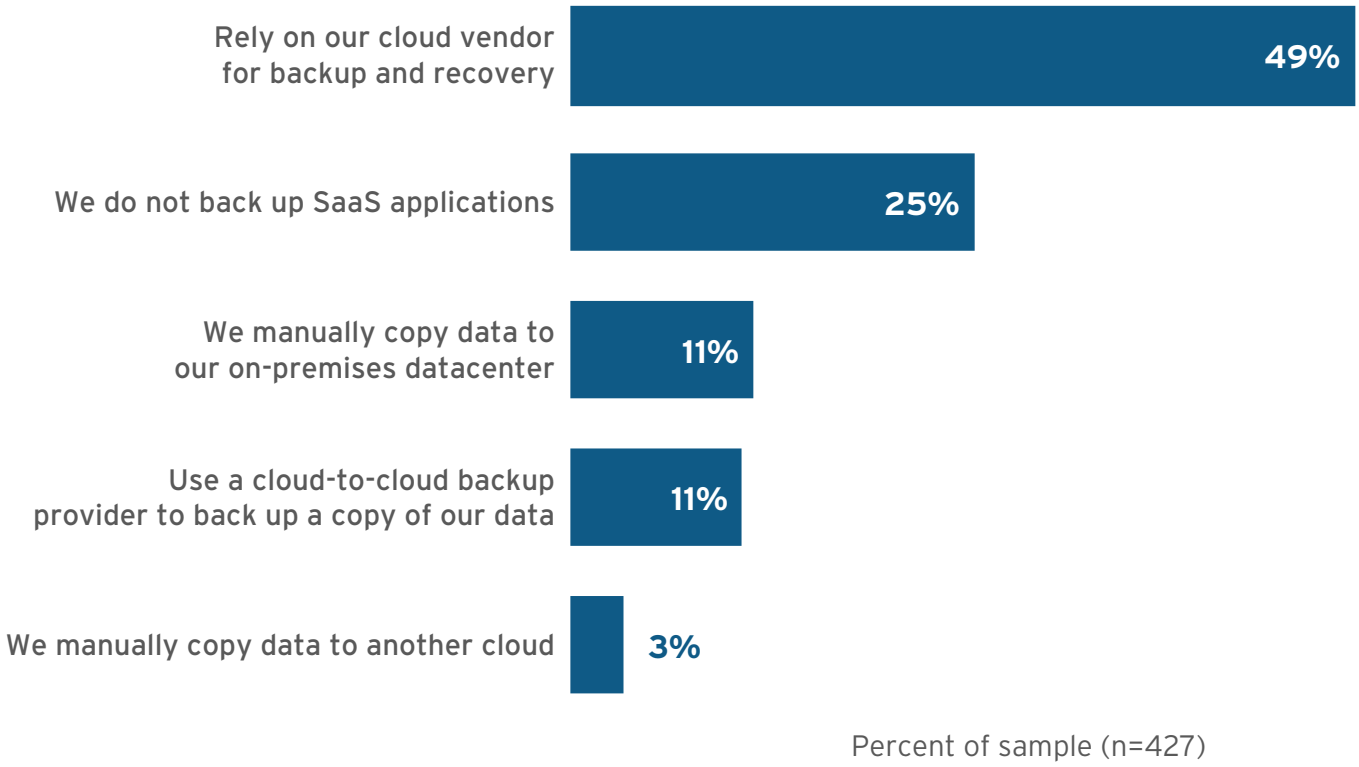
SaaS Data Backup in the Public Cloud – Out of Sight, Out of Mind?

Data backup remains one of the key principles in data protection for several reasons, and while SaaS vendors focus on providing infrastructure resiliency and application availability for their own platform, the traditional 3-2-1 backup rule still applies as a best practice for ensuring data protection and resilience. With SaaS data, the dynamics change because the original data may have been created and only exist on the SaaS vendor's cloud storage platform and should be backed up to a second, independent location – either to a separate IaaS cloud storage target or on-premises if dictated by industry-specific compliance requirements.

Tier one cloud datacenters are designed to provide top-level, 24/7/365 availability, security and resilience, but even with that remarkable degree of engineering, most cloud vendors themselves still recommend a model covering multiple datacenters and/or availability zones to protect against outages. The problem is that the replication-based model they use to protect their own systems is not the same as an independent backup of your SaaS data. 451's VoTE polling results below illustrate the inconsistencies in the ways customers protect and manage SaaS-generated data.

Figure 2: SaaS data protection

Source: 451 Research's Voice of the Enterprise: Storage, Budgets and Outlook 2017
Q: What is your organization's primary data protection strategy for SaaS applications?



Out of the five options listed in Figure 2, only 11% of the respondents come close to addressing the primary need for a consistent and automated backup. While it is not required that the backup be with a cloud-to-cloud backup provider, it is critical that it be independent of the cloud platform itself**.** Manual copying of any type can be inefficient and prone to errors, and the 25% that don't make any backups at all are playing a dangerous and potentially costly game. The highest percentage of responses trust their cloud vendor to do backup and recovery, but this is only a viable option if a SaaS vendor specifically offers full backup and recovery services. Most do not, and this misunderstanding can pose a major risk to business-critical data. It ultimately comes down to the best-practice rule that data should be backed up to a second system/location, be it cloud to cloud or cloud to on-premises.

Office 365 and the Growing Significance of this Business-Critical Data

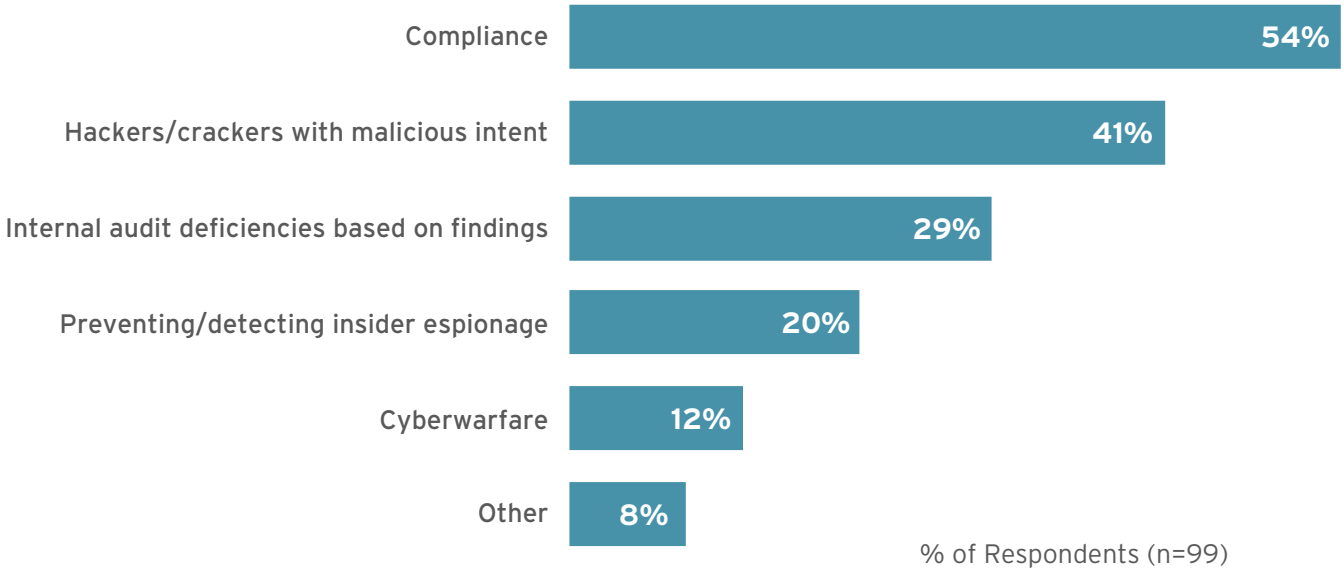
Historically, databases have been the top priority in the BC/DR equation, and rightfully so. As the primary application environment for conducting business, databases are the logical focus for data protection, but times are changing. Today's business environment increasingly depends on the documents, emails and other business-critical information that is created, stored and shared within the Office 365 SaaS dataset, and this type of information is making up a growing majority of the on- and off-premises data that's being generated and stored as a critical part of modern business.

It's easy to think that all data protection is alike, but there are major differences between protecting the Office 365 infrastructure and protecting customer data created and stored in Office 365. This makes it critical for IT to help establish the relative business importance of Office 365 data in order to assign appropriate data protection and governance. And while the collaborative flexibility offered by shared SaaS storage is a positive, it only makes it more important for IT to help ensure that there is sufficient security to protect against a targeted intrusion.

This hole in data protection isn't lost on cybercriminals who are now actively focusing ransomware attacks and other disruptions that can leverage the vulnerability gaps between the responsibility of the SaaS vendor and the organizations that own the data, nor does it escape the attention of industry regulators who are increasingly focusing on data security. In 2018, a 451 VoTE security survey asked enterprise customers what their key security concerns were over the last 90 days, and it was telling to note that concerns about industry compliance exceeded those of threats with malicious intent.

Figure 3: Top information security concerns within last 90 days

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2018
Q: What were your top general information security concerns during the last 90 days?



Most of these security concerns align almost exactly to the most common vulnerabilities for Office 365 and other shared data environments, but these risks can be substantially reduced by a data protection schema based on the classic 3-2-1 rule for data backup and scheduled to meet appropriate RTO/RPO requirements. Office 365 data that primarily resides in the cloud offers convenience and relatively high availability, but best practices still dictate that it should at least be backed up to a public cloud provider such as Azure or AWS, or alternately, on-premises to ensure greater accessibility and control.

This points to the most important reason why you have a backup, which is data recovery. An Office 365 backup offers data loss protection, but that can be of little value if data recovery is limited by factors such as bandwidth, connectivity, recovery granularity, failed backups or the inability to recover to an alternative destination or format. IT administrators who focus on data protection – especially in the context of Office 365 data – are often tasked with a complex set of challenges when it comes to recovering specific data from a massive repository of backups, or the need to recover complete Office 365 datasets after a ransomware attack. But administrator responsibilities can also be as mundane as recovering a specific email or file for a user, so having the right tools to do this as quickly and efficiently as possible frees up valuable time that could be used for more important business tasks. As a rule, any Office 365 backup strategy should have a matching recovery strategy that addresses data loss vulnerabilities both large and small, provides granular and directed recovery options, and includes a testing schema that evolves as changes are made in infrastructure, platform or RTO/RPO requirements.

Office 365 Archiving, Governance and E-discovery

While very similar, backups and archives are not the same, and they should be approached with different goals in mind. In the case of Office 365, SaaS data archiving provides a model for transitioning and managing older, less frequently accessed data to a separate tier. While this archiving offers a model for setting up rules-based data workflows and convenient way to extend Office 365's online storage capacity, it's not a replacement for regular backups. And though the data in those archives may change more slowly, it remains important to ensure that archived data is also protected by a 3-2-1 backup strategy.

The newest risk for SaaS data comes from challenges created by privacy initiatives such as GDPR and the California Consumer Privacy Act of 2018, which is scheduled to take effect in 2020. GDPR became law in 2018 and applies to the processing of personal data from any business activity in the EU without regard to whether the processing occurs inside or outside the EU. The regulation gives EU residents more control over their data. Individual powers include the ability to prohibit data processing beyond its specified purpose for collection, the right to be forgotten, and the ability to withdraw consent to the collection and use of personal data.

This can become a serious problem that is only made worse by the colossal amount of legacy data that's been piling up across the industry. Appropriately protecting and managing all these emails, documents and sites can be a daunting task, but from a business perspective, it won't be long before the risks of *not* managing personal data could far exceed the cost of fixing the problem if found in violation. The GDPR alone has penalties of up to €20m or 4% of a company's annual revenue, whichever is higher, for infraction. In the US, the proposed California Consumer Protection Act of 2018 adopts a somewhat different model based on a $7,500 fine for each violation. To put this in perspective, a CCPA violation affecting 500,000 accounts could potentially result in a fine of $3.75bn.

Another legal consideration that drives SaaS data protection is the e-discovery process that companies must undergo as part of a legal action. When a company receives a subpoena for business data, that data suddenly becomes evidence, which changes everything. Depending on the scope of the request, it then becomes the company's responsibility to identify, preserve, collect and process that data to present to its legal defense team, who will then review and analyze that data for relevance and context, exclude privileged information and then prepare it for submission to the court. A legal hold is a process for locking down data to ensure it's not deleted or modified in the process, and it's important to have the tools necessary to meet the granular protection and security needs of an e-discovery event. But a legal hold is something that needs to be used selectively, and though Office 365 offers broad legal hold capabilities, a full and independent backup copy of SaaS data may be the best approach for providing a point-in-time dataset for e-discovery purposes. Unfortunately, the rules of evidence can vary substantially between jurisdictions, so a company should always refer to legal counsel before responding to a court order for digital evidence, and then follow that advice to the letter.

Legal and otherwise, we believe that there will be a steadily growing need for businesses to gain better visibility and greater control of their cloud and SaaS-related data. Office 365 offers a mix of convenience and flexibility for business customers, and combining that with an appropriate data protection model only makes sense as Office 365 SaaS-based storage options continue to gain traction in the business community. A truly hybrid cloud approach should look at public cloud services and resources as an extension of an on-premises infrastructure, and cornerstone principles related to data protection, business continuity and disaster recovery do not evaporate simply because an application is running in the cloud.

Conclusions/Recommendations

When it comes to applications like Office 365, SaaS providers offer reasonable assurances that they are protecting the underlying infrastructure to meet their contractual SLAs, but that protection doesn't extend to customer data created on those platforms. It's critical for customers to find solutions to protect their own data from risk – and based on their own terms rather than on the potential limitations of the SaaS platforms offerings. The challenge for IT organizations is to understand the vulnerabilities associated with data residing on SaaS platforms, and ensure they have the proper solutions in place to ensure protection, control and accessibility. These are some of the key actions to take when considering protection of Office 365 data.

- **Know that Microsoft provides infrastructure resiliency and application availability within Office 365, but you are the data owner.** You are responsible for the protection of your own business data, and you should define data protection based on the specific needs of your business.
- **Research and consider acquiring a third-party data backup solution.** It's one of the best ways to cover your business from data loss vulnerabilities related to Office 365. Plan to address threats such as accidental deletion and internal and external security threats, and to meet mandated security or compliance requirements.
- **Engage stakeholders in your business (and within your IT department) to set and test data recovery SLAs.** Test various data recovery scenarios within native SaaS platform tools and compare those with third-party backup products.
- **Understand the specific compliance and legal rules of your business environment**. The laws surrounding data protection and security are always changing, and one of the key considerations of any data protection plan should be ensuring compliance.

About 451 Research

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

NEW YORK
1411 Broadway
New York, NY 10018
+1 212 505 3030

SAN FRANCISCO
140 Geary Street
San Francisco, CA 94108
+1 415 989 1555

LONDON
Paxton House
30, Artillery Lane
London, E1 7LS, UK
+44 (0) 203 929 5700

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

451 Research®