Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **April 2019**
Sponsored by **Druva**

Filling the Gaps in Office 365 Data Protection

Executive Summary

Office 365 is a robust and capable cloud service that does a wide variety of things for a mass-market audience and provides useful security, compliance, productivity and data protection capabilities. In the areas of data protection and security, it can be argued that Microsoft has done more to protect user data than any other SaaS provider. It is also true that third-party companies that specialize in these areas can perhaps provide even more protection for Office 365 data.

Furthermore, the use of third-party solutions will often enable the use of less expensive Office 365 plans, as well as a reduction in the use of storage beyond the initial allotment provided in a given plan, resulting in a total cost of ownership that can be lower than if only more expensive Office 365 plans are used. For example, based on just list prices, the use of Office 365 Enterprise Plan E3 will save an organization $15.00 per user per month compared to the use of Enterprise Plan E5, a total savings of 43 percent. There are several security, data protection and archiving services that could be combined from various third party solutions to supplement the native capabilities in Office 365 for less than $15.00 per user per month, resulting in a net savings relative to the cost of Plan E5.

ABOUT THIS WHITE PAPER

This white paper was sponsored by Druva. Information about the company is offered at the end of the paper.

Office 365 Has Been Successful

Microsoft has been pursuing "cloud" offerings for many years, starting with hosted Exchange in the late 1990s, followed by BPOS, and now Office 365. In this third iteration, Microsoft has clearly hit its stride: as of October 2018, Microsoft reported 155 million customers for the platform, up from just 60 million just under three years earlier. In short:

- **Office 365 offers a number of useful capabilities**
  Office 365 includes business-grade email, desktop productivity capabilities, file sync-and-share, collaboration tools, voice communications, instant messaging and a range of other capabilities in a variety of packages at different price points. Microsoft has tailored its offerings to a wide range of customers and offers services aimed at specific industries.

- **It's becoming the dominant business platform**
  Microsoft, as a "cloud-first" vendor, has been making a concerted push to move its customers of on-premises solutions to the cloud, with the result that most Microsoft business email customers are now using Office 365 and not on-premises Exchange. While Microsoft has dominated the on-premises email market for many years, it is now doing so to an even greater extent in the cloud.

- **Microsoft has done a good job at providing a good set of solutions**
  Overall, Microsoft has done quite a good job at assembling a wide range of solutions for a broad audience, and has provided decent security, archiving, encryption, data protection and other capabilities to support them.

SOME THINGS CAN IMPROVE

Despite the appeal and utility of Office 365, there are some areas of functionality where things can be improved:

- **Malware protection**
  Most organizations that use Office 365 rely on the basic security that is offered natively in the platform. For those using a version of Office 365 with the more

Despite the appeal and utility of Office 365, there are some areas of functionality where things can be improved.

capable Microsoft Advanced Threat Protection (ATP), security is better, but it does have some limitations. For example:

- The only way to get a consolidated view of threats is to use Cloud App security, which is available only in the Plan E5 subscription.
- The spam quarantine does not share information with users on how many similar messages were received with a similar subject line and sender by other users in the organization. A higher number might signal the likelihood that the message is spam or a phishing attempt. This intelligence could help users make more informed decisions about the likelihood that a message might be carrying malicious content.
- Safe Attachments uses virtual sandboxing to assess the presence of malware and other threats in a document. This approach is not effective against certain types of threats like password-protected ransomware sent with the password in the body of the email. Competitive offerings go beyond sandboxing on virtual machines, and include the next-generation of advanced detection mechanisms, such as deep content inspection, recursive analysis of embedded documents, evaluation of threats below the application and operating system levels, identification of dormant code, sandboxing on controlled physical machines to analyze for malware that evades virtual sandboxing detonation, and more. Microsoft's ATP is not on par with some best-in-class, advanced, third party offerings on the market.

- **Data protection**
  Among the limitations in Office 365's data protection approach are:
  - Accidental deletion protection relies on the Recycle Bin, which can be accidentally or maliciously cleared; or on Retention Policies, which are complicated (there are 25 pages of documentation to describe them.)
  - Retention Policies result in a significant increase in storage use within SharePoint and OneDrive, possibly resulting in having to pay for extra storage beyond what is included in a given plan once the storage allocation has been consumed. Additional storage is priced at $0.20 per gigabyte per month, meaning that an additional 50 gigabytes of storage per user in a 1,000-user company will cost $10,000 per month.
  - Retention Policies alone do not protect against rogue administrators unless Retention Lock is added. However, this feature cannot be disabled once it is turned on, and so organizations that experience a major increase in storage will not be able to rectify that problem by disabling Retention Lock.
  - The "3-2-1 Rule" (three copies of data, two on different platforms/media, one in a remote location) is a well-established best practice for data protection. However, the native capabilities to protect data within Office 365 use the platform itself to provide data protection, a violation of the 3-2-1 Rule. The use of an external service or platform to protect Office 365 data is much more in line with best practices – and is recommended by Microsoft itself in its service agreement.
  - Office 365 offers some capabilities for recovering corrupted data. For example, Files Restore reverts OneDrive to a specific point in time from the past 30 days. It reverts all basic file and folder operations that transpired during the selected time period, but does not support a selective restoration. For selective restoration – for example, to recover a file or folder that was deleted accidentally rather than being subject to a ransomware attack – OneDrive offers access to the Recycle Bin for selective restoration, and/or Version History for each file to roll back to a previous version. The

The native capabilities to protect data within Office 365 use the platform itself to provide data protection, a violation of the 3-2-1 Rule.

ability to restore files, folders, and subfolders is a very standard feature in third party backup tools.

- SharePoint sites and subsites can be restored, but this must be done by Microsoft support, and there are a number of major limitations with this service. These include the fact that there is no service level agreement (SLA) for it. If a site collection needs to be restored, Microsoft can only restore the entire site in place, but any data created after the latest backup will be lost. They can restore subsites to alternate locations, but Microsoft says this process is more complicated and error-prone than a full site collection restore.

- **Long-term archival of data**
  SharePoint content, such as documents and list items, can be retained in place through retention policies, or moved to another location in SharePoint when it has expired or has become irrelevant. What is not possible, however, is to archive SharePoint content that is no longer current to alternative and cheaper storage systems. Although it is possible to purchase unlimited SharePoint storage capacity, it also attracts premium pricing ($0.20 per gigabyte per month) as noted earlier.

  Office 365 data will be retained for three years and deleted afterwards, deleted emails will be moved into an archive folder and held there for three years, after which they will be deleted. It is important to note that the total retention period will be three years, not three years in mainline storage and an additional three years in an archive folder.

  The Office 365 Audit Log retains audit events for only 90 days and there is no way to increase this time frame (although Office 365 Enterprise Plan E5 provides one year of storage). This has significant implications for organizations that must comply with legal or regulatory retention requirements that demand retention of this data for much longer periods.

- **Content from departing employees can be retained**
  Microsoft's inactive mailbox facility has enabled leaver's mailboxes to be retained indefinitely without charge, but inactive mailboxes may attract new licensing terms and higher costs than exist with the current retention policy. Given that roughly one-quarter of employees leave their employers annually, the costs associated with departing employees – and maintaining and protecting their content – is an important consideration.

- **Import can corrupt a mailbox**
  An import can accidentally corrupt a mailbox. For example, if a .PST file has been imported into a mailbox, it is not possible to remove just the imported emails or to do a point-in-time restore to a point prior to the .PST import. A user in an online forum recently posted this exact scenario, including the difficulty in cleaning it up without the ability to do a point-in-time restore.

- **Users on legal hold**
  If a user is on legal hold, their deleted email is not automatically migrated to an archive folder, but is instead put into the "dumpster". If the dumpster exceeds 100 gigabytes, it must be manually moved to an archive folder or another retention policy must be established to handle it.

COMPLIANCE

Compliance has always been a critical issue for more heavily regulated industries, such as financial services, healthcare, energy and government. However, with the advent of privacy regulations like the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) – among a growing number of other such regulations – compliance is now an issue for the vast majority of organizations, regardless of the industries in which they participate. Good

Compliance has always been a critical issue for more heavily regulated industries.

compliance means being able to identify sensitive and unstructured data, and also centrally managing policies for compliance that span multiple services. Office 365 has some limitations in its compliance capabilities:

- **Regulatory considerations – supervision**
  Financial Industry Regulatory Authority (FINRA) Rule 3110 requires certain individuals, such as registered investment advisors, have their communications supervised for compliance with Securities and Exchange Commission and FINRA requirements. The goal is to sample these communications to determine if there are potential violations of the applicable rules that govern them.

  Office 365 includes supervisory capabilities: in May 2017, Microsoft's Supervisory Review capability was replaced with a new Supervision tool that necessitates use of Enterprise Plan E5 or the Advanced Compliance add-on. In January 2019, a new version of the supervision tools was announced, but Plan E5 or the Advanced Compliance add-on are still required.

- **Regulatory considerations – privacy obligations**
  In 2018, there was a dramatic shift to privacy regulations beyond traditional data security mandates. With it came the expectation of being able to handle search (subject access requests) and the right to be forgotten (discovery and deletion). While Office 365 has basic functionality to support these requirements, the burden is still on IT to fulfill them through IT-centric processes and admin interfaces. Therefore, organizations need to be prepared to have IT disrupted by requests that really should be delegated to legal or line-of-business owners. Third party tools are available to support this compliance requirement and prevent it from becoming an IT bottleneck. Moreover, content that is subject to a retention-lock period cannot be deleted, even if statutory requirements like the GDPR or CCPA require it. The only way to reduce the retention period of new emails is to a) create a new policy with a reduced period, b) deactivate the old policy, and c) activate the new policy. The new policy will only apply to newer files and emails; old data will continue to be retained for the period specified in the previous policy.

- **Legal considerations**
  Some reasonably sound eDiscovery capabilities are included in Office 365, but these have some limitations. For example:

  - There is no workflow or project tracking.
  - Microsoft does not offer a Service Level Agreement (SLA) for a Content Search or eDiscovery search, but claims that 100 mailboxes can be searched in 30 seconds and 10,000 mailboxes in four minutes. Osterman Research has found that, in practice, searches take much longer to return results. A third-party tool specializing in such things can do this much faster than Office 365's native capabilities.
  - Searches for keywords that are started in the Content Search tool cannot be imported into an eDiscovery case in a way that can be tracked and defended from a legal perspective.
  - Separate retention, preservation and disposition policies cannot be created for a user's mailbox and their Online Archive. What's defined for one is defined for both, a limitation for organizations that want to define separate policies.
  - There is no provision to create a case template for repeatability and auditing, without the use of PowerShell.
  - eDiscovery cases in Office 365 are blind to post-export actions that may need to be defended in court.

Some reasonably sound eDiscovery capabilities are included in Office 365, but these have some limitations.

While Microsoft has recently announced the rollout of new capabilities to its Advanced Discovery service, these capabilities are not available in the base eDiscovery offerings and require the use of Enterprise Plan E5 or an add-on. Moreover, the new capabilities do not address all of the weaknesses and limitations of earlier eDiscovery capabilities.

Next Steps

When considering the deployment of Office 365, Osterman Research recommends that decision makers take the time to fully analyze the capabilities and limitations inherent in the platform.

DUE DILIGENCE IS ESSENTIAL

Multiple Osterman Research surveys conducted with organizations that have deployed Office 365 have found that the decision to move to the platform is quite often a top-down decision. Architects, security decision makers, compliance managers and other key stakeholders often are not consulted before the decision to move to Office 365 is made. The result is that most of those charged with deploying and managing Office 365 will know the platform at a high level, but are not familiar with the minutiae of what the platform will and will not do, and how it differs – sometimes substantially – from the processes and technologies that were in place before. We found that "getting into the weeds" of Office 365 can be a laborious process.

THE LIMITATIONS IN OFFICE 365 NEED TO BE UNDERSTOOD PRIOR TO DEPLOYMENT

In the context of data protection, Office 365 relies on itself to protect customer data. However, it is essential for decision makers to understand the importance of not having all of their data stored in the same place, since the "old school" rule of 3-2-1 breaks if all data is stored in the repository or service. Using multiple, independent repositories is an essential element of data protection and a best practice that every organization should follow.

It is essential for decision makers to understand the importance of not having all of their data stored in the same place.

AN ACCURATE COST ANALYSIS IS ESSENTIAL

A key element of any due diligence process for Office 365 is a thorough cost analysis of the platform over time. Some Office 365 customers opt for the "full meal deal" in Office 365, assuming that the Enterprise Plan E5 (with a list price in the United States of $35 per seat per month) will offer the array of data protection, archiving, security, compliance and other capabilities they will require. Others choose to stay with Enterprise Plan E3, but purchase add-ons such as Advanced Threat Protection, Advanced E-Discovery and Cloud App Security, making E3 more expensive. However, Osterman Research has found that the use of third-party solutions in conjunction with a less expensive Office 365 plan (e.g., Enterprise Plan E3 with a list price in the United States of $20 per seat per month – without extra-cost add-ons) will offer better capabilities than what is available with Plan E5 and at a lower total cost per month. The key capabilities for which third-party solutions should be considered include:

- Malware protection that includes all emails and files stored in OneDrive and SharePoint.
- Immediate malware remediation through customer-initiated point-in-time restore of any object, including a single file, a folder, an entire user's mailbox, SharePoint account, or OneDrive folder – without need of support.
- Data protection, including storage of Office 365 data on a non-Microsoft platform; and capabilities to recover corrupted data and individual files.
- Protection of your data while allowing you to delete individual records from your Office 365 account to comply with regulations like GDPR's Right-to-be-Forgotten.

- The ability to archive key content types, such as SharePoint and OneDrive data.
- Supervisory review capabilities for organizations in heavily regulated industries, such as financial services.
- eDiscovery capabilities that provide robust workflow and project tracking capabilities, SLA for search, and more granular eDiscovery capabilities.

Summary and Conclusions

Office 365 is a good offering that will satisfy a number of business requirements for security, archiving, data protection, encryption and other essential business processes, but it has some feature and function gaps that must be well understood before deployment. Many third-party solutions will do a better job at filling these gaps and should be evaluated and considered by decision makers.

About Druva

Druva delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; delivering globally accessible, infinitely scalable and completely autonomous enterprise data resiliency. Customers drive down costs by over 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva's patented cloud architecture transforms backup data into an asset, making it more open and accessible so customers can streamline governance, improve cyber resiliency, and gain critical insights to uncover opportunities and expedite decision making.

Learn more about data protection and management for the cloud era at www.druva.com.

Office 365 is a good offering that will satisfy a number of business requirements… but it has some feature and function gaps that must be well under-stood before deployment.