WHITE PAPER

Filling the Gaps in Office 365

An Osterman Research White Paper
Published October 2017

Viewpointe

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond • Washington • 98010-1058 • USA
+1 206 683 5683 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

EXECUTIVE SUMMARY

The title of this white paper notwithstanding, Osterman Research wants to make it clear at the outset that we believe Microsoft Office 365 to be a robust and capable platform, one that will serve most organizations well. If your organization is using Office 365, we recommend you continue to do so. If you're not using it, we recommend you consider it. Microsoft offers a large, varied and growing number of features and functions in Office 365, and at a wide range of price points that will satisfy a number of different markets.

That said, decision makers evaluating the efficacy of Office 365 to meet their business requirements must be aware of its shortcomings in the areas of data protection, archiving, security, encryption, authentication and eDiscovery (among others) covering workloads like Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, and Azure Active Directory. An awareness of these shortcomings enables decision makers to plan for the mitigations required to assure the proper business performance of Office 365.

KEY TAKEAWAYS

- Office 365 is proving to be an enormously successful offering for Microsoft and will be employed by roughly 120 million users by the end of 2017.

- Office 365 bundles a large number of capabilities into a single offering for worker productivity, supported by a backdrop of data protection, archiving, security, encryption, compliance, and eDiscovery tools for the modern organization. Microsoft offers a large number of different plans designed to allow organizations to "rightsize" specific plans with various user roles and requirements, enabling decision makers to choose the right plan for individual user groups.

- While the tools in Office 365 provide good capabilities in certain situations, the Office 365 approach to data protection, archiving, security, encryption, compliance, and eDiscovery are not necessarily best in class, nor will they address all the needs of the modern organization. It is important to note that while the native capabilities in Office 365 will generally meet the needs of smaller, less complex and less heavily regulated organizations; it becomes more difficult for these capabilities to meet the needs of larger, more regulated and more heavily litigated organizations.

- The risks of relying solely on Office 365 are significant, such as when a phishing or new-variant ransomware email is not detected by its security toolset. In short, organizations should avoid putting all of their eggs in one basket. They should diversify threat intelligence and mitigation strategy with a multi-layered defense approach.

- Office 365 is a fast-changing offering, and while that potentially offers great new value for customers, it also makes it extremely difficult to know what is currently available in Office 365 and for which plans. There is a great deal of confusion as to available capabilities, and customers are likely to find capabilities they thought were available require an additional cost add-on from Microsoft or a higher-level plan. In short, decision makers should not assume that Office 365 includes all of the services they will need to properly manage their data.

Decision makers should not assume that Office 365 includes all of the services they will need to properly manage their data.

ABOUT THIS WHITE PAPER

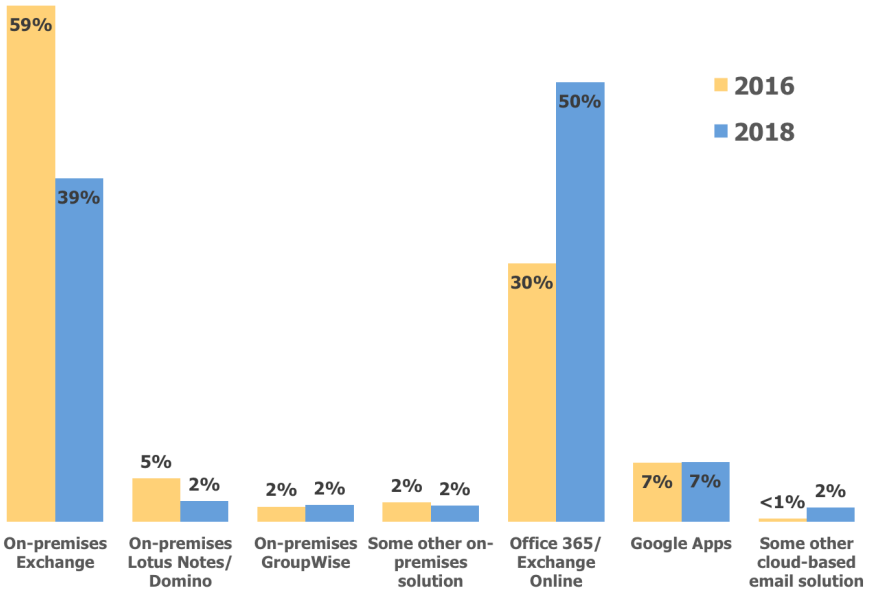
Osterman Research conducted an in-depth survey of organizations that are migrating to Office 365, have already done so, or will be doing so within the next 12 months. We present some of the results of that survey in this white paper, but will be publishing a report of the survey results shortly after publication of this white paper.

This white paper was sponsored by Viewpointe – information on the company is provided at the end of this paper.

THE MOVE TO OFFICE 365

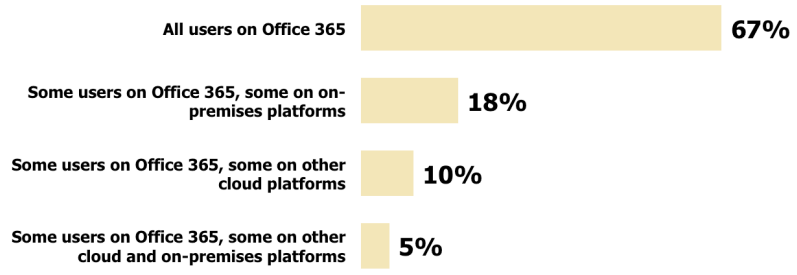
Microsoft's success with Office 365 is undeniable: in April 2017, the company reached the 100 million-user milestone for Office 365 and will likely reach about 120 million users by the end of 2017[1]. Our own research, as shown in Figure 1, clearly demonstrates growth in the adoption of Office 365, as well as the significant shift that is occurring away from on-premises Exchange. Interestingly, however, among organizations that are migrating, will migrate, or have already migrated to Office 365, about two-thirds will not migrate completely to Office 365, but will continue to use other platforms, as shown in Figure 2.

Figure 1
Users by Email Platform, 2016 and 2018



Source: Osterman Research, Inc.

Figure 2
Plans for Use of Email Platforms Once Office 365 is Fully Deployed

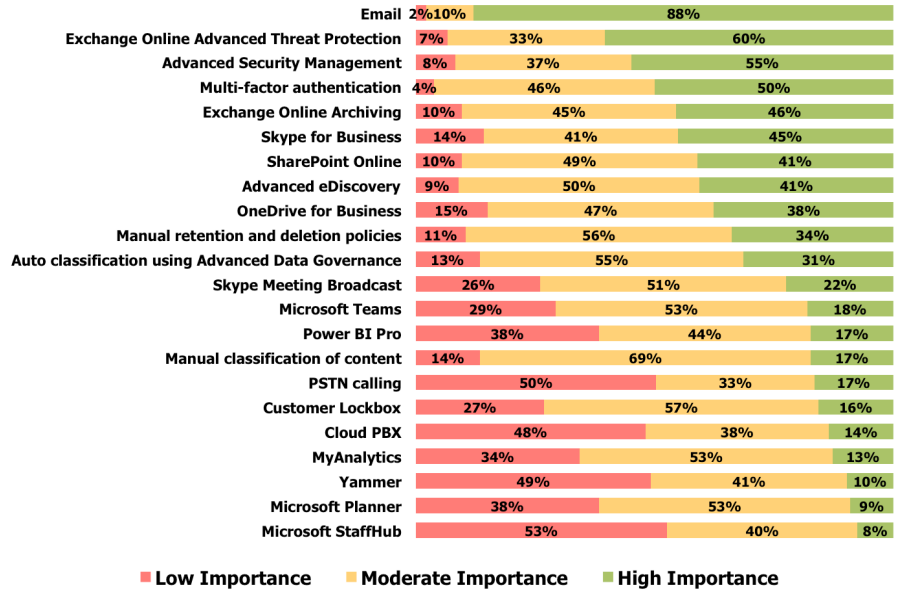


Source: Osterman Research, Inc.

[1] https://www.petri.com/office-365-hits-100-million-users

Our research discovered that organizations moving to Office 365 are focused on a wide range of Office 365 solutions and capabilities, but the features and capabilities that are most important are email, security, multi-factor authentication, archiving, and telephony/real-time communications, as shown in Figure 3.

Figure 3
Importance of Various Office 365 Solutions and Capabilities



Source: Osterman Research, Inc.

Given that one of the benefits of migrating to Office 365 or any other cloud-based platform is the potentially lower cost of ownership for cloud services, one of the key issues that decision makers must address is how best to drive down its cost. For Office 365, a key issue then becomes the means by which to minimize the costs of ownership:

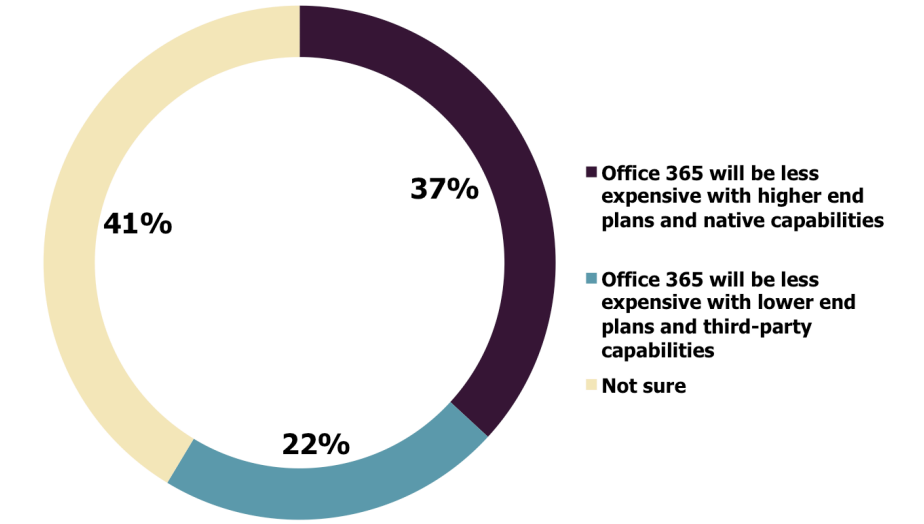
- Treat Office 365 as a "one-stop-shop", employing more expensive plans with all of the features and functions that users require, or
- Use less expensive plans and supplement the missing capabilities with third-party offerings.

While Osterman Research recommends the latter approach, as will be clear after reading this white paper, much of the market for Office 365 is still not sure which approach to take. As shown in Figure 4, 22 percent of organizations plan to use less expensive Office 365 plans and supplement the native capabilities with third-party solutions, 37 percent will use high-end plans, but 41 percent simply are not sure.

It is important to note that even the "one-stop-shop" approach to Office 365 really won't work for organizations of medium or greater complexity, since virtually no complex cloud-based or on-premises platform is optimal without the addition of third party capabilities.

Our research discovered that organ-izations...are focused on a wide range of Office 365 solutions and capabilities.

Figure 4
Views on the Cost of Office 365 with and without Third-Party Solutions



Source: Osterman Research, Inc.

ARCHIVING AND CONTENT MANAGEMENT LIMITATIONS

The majority of organizations embracing Office 365 use it in addition to other cloud-based and on-premises infrastructure and content-creating applications. This creates an additional set of content sources and content types that need to be secured, controlled and governed, often under changing conditions and constraints as Microsoft morphs the Office 365 service and its capabilities. While Office 365 offers ever-expanded and potentially unlimited storage capacity, keeping all content forever is not a sound business, legal, or information management decision. Information becomes expensive – unnecessarily so – when:

- Out-of-date or obsolete information causes confusion. Search results return information that is no longer valid, and if shared, the misinformation just spreads. People make decisions based on poor intelligence. Content that is no longer necessary gets in the way and slows the ability to find and retrieve the correct and desired information. The organization's information landscape becomes cluttered and ineffective.

- Content that contains Personally Identifiable Information (PII) or that is subject to regulations like the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), or the Payment Card Industry Data Security Standard (PCI DSS) cannot be not managed properly.

- Information held beyond its useful life raises legal retention issues in the case of potential or actual litigation. The process of searching, identifying, reviewing, tagging, and producing content for eDiscovery increases as the amount of stored content increases.

In exploring the capabilities of Office 365, organizations need to examine how best to balance business, compliance, records, legal and IT goals. Decision makers should be aware of the following limitations in the data protection, archiving and content management capabilities in Office 365.

NO ARCHIVING FOR SOME CONTENT TYPES

Office 365 does not offer full-fidelity archiving (i.e., retention of all of the content's attributes) for certain content types, such as SharePoint, Skype for Business, additional message types and third-party content. Specifically:

- SharePoint content can be retained in place through retention policies, or moved to another location in SharePoint when it has expired or become irrelevant. The actions can be triggered based on a couple of specific date-based event triggers only, and if organizations stay within their storage limits for SharePoint, In-Place Records Management in SharePoint may be sufficient. What you can't do, however, is push SharePoint content that is no longer current to cheaper storage systems, and while unlimited SharePoint storage capacity is available to purchase, it is priced at the premium end of the scale. Organizations with large quantities of data that want to keep their SharePoint content trimmed and current without incurring additional storage fees over the long term, or who want to archive content out of production based on event triggers beyond date-based metadata, are poorly served.

- Skype for Business Online does not offer a native archiving capability, relying instead on Exchange Online if certain conditions are met. Instant messaging transcripts are retained in each user's Conversation History folder in their Exchange Online mailbox, but unless the mailbox is on hold, the user can delete their messages at will (as they also can in SharePoint). To force the retention of messages, a user's mailbox must be on In-Place Hold; by implication, to force the retention of all Skype for Business Online messages, all mailboxes must be on hold at all times. If a mailbox is on hold, peer-to-peer and multiparty instant messages are retained, as well as content upload activities during meetings. Other actions within Skype for Business are not retained, such as peer-to-peer file transfers, audio/video for peer-to-peer instant messages and conferences, application sharing, and conferencing annotations.

- Text messages cannot be archived into Office 365, with the exception of text messages on BlackBerry devices, and only if there is a third-party agreement in place to capture such messages. With BlackBerry currently having an extremely small market share – iOS and Android dominate the market – the integration option doesn't give organizations much value.

- Content from third-party messaging, collaboration, social media and other content services can be archived only if there is an agreement with a third-party data partner, and all content is converted into an email message to be stored via Exchange Online in the mailbox of a specific user or a catch-all mailbox. Archiving is not full-fidelity according to what actually happens in the original service, which makes re-creating a historical chain of events very difficult.

Skype for Business Online does not offer a native archiving capability, relying instead on Exchange Online if certain conditions are met.

ENCRYPTION

Office 365 offers an email encryption service, called Office 365 Message Encryption as part of the higher-cost Enterprise plans, and available as an additional cost add-on to other plans. It is designed to enable an Office 365 user to send encrypted email to any recipient without having to know what email service, email client, or encryption capabilities they support. Office 365 Message Encryption (or OME for short) supports messages up to 25 megabytes in size, and sends the message as an encrypted HTML attachment that can be viewed only using the Office 365 viewing portal. OME is powered by the Azure Rights Management Service.

Microsoft does not offer a transparent end-to-end encryption service that will automatically encrypt and decrypt messages for both senders and recipients without additional per-message steps and authentication requirements.

Encryption is triggered by a policy set using an Exchange transport rule configured by an administrator. The policy trigger can require a manual action by the sender, such

as adding the word "encrypt" to the subject line, although manually triggered encryption is less than ideal. The policy trigger equally can be something more automated, such as the recipient being outside the firm and the message containing certain words or phrases.

When an encrypted message is received to a desktop or laptop, the recipient must save the HTML attachment, open it in a supported browser, and login either using an Office 365 or Microsoft account, or gain access via a one-time passcode. On an iOS or Android mobile device, Microsoft offers a viewer app for OME messages, and on other mobile devices, the HTML attachment must be opened in a supported browser, with the same authentication options for the desktop user.

These steps are required even for other Office 365 users using Outlook 2016 for Windows, the premier and most advanced email client offered by Microsoft. There is no support for fully transparent and seamless delivery of encrypted messages between Office 365 subscribers in different organizations.

While OME is an admirable attempt to address the challenges of email encryption in a heterogeneous email world, it suffers from numerous shortcomings that undermine the proposition:

- OME is blind to what happens after the message is sent, and therefore messages cannot be revoked, nor is there reporting available on what happened to the message. The user does not know if the message has been received – even through special actions are required to access the message – and administrators likewise have no visibility into read status.

- The original subject line is delivered for an encrypted email message; you can't rewrite the subject line to something generic. The subject line could include sensitive or confidential information that needs to be protected, not just the email body.

- Because OME is a server-side encryption process, the original copy in the user's Sent folder is stored unencrypted.

- The HTML attachment must be downloaded or saved before it can be opened; if it is opened directly, the sign-in part of the message is hidden. This is confusing for recipients.

- The one-time passcode is sent ONLY by email, to the same address as the message was delivered. There is no other way to send it, to get around a compromised account.

In summary, the additional steps required for reading and replying to such messages means that OME is built for infrequent encryption of email; it is not designed nor implemented to provide encryption for all message traffic, or even most message traffic.

At Microsoft Ignite in September 2017, Microsoft announced a new option for applying encryption: the Do Not Forward permission in Outlook, in addition to other custom templates to automatically apply encryption. However, these capabilities still require a user action (i.e., checking the box of "Do Not Forward"). Admittedly, this is easier than typing "encrypt" in the subject line, but it still requires manual intervention. Moreover, Microsoft also announced at Ignite that Office 365 users can now read and reply to encrypted messages natively within Outlook (desktop, Mac, web, iOS and Android mobile), and that non-Office 365 users can authenticate and read protected messages using their Google or Yahoo! identities.

INDEXING FILE TYPES

Office 365 can index a specific list of 58 file types, which is weighted heavily in favor of the various file formats in Microsoft Office products. When undertaking an

eDiscovery search and performing an early case assessment, any file that is not included in the 58 will be flagged as unprocessed. When applying Data Loss Prevention (DLP) rules, file types not included in the 58 will not trigger the capture rules. The implication is the need for a manual review of these non-supported file types by a compliance or security officer, adding cost and decreasing timeliness of information exchange. If an organization makes regular use of non-supported file types, it should look at third-party tools that will index additional file types.

LITIGATION HOLD CAPABILITIES

Microsoft offers a range of evolving capabilities for litigation or legal hold in Office 365. Historical approaches have been linked with specific workloads, such as Exchange Online and SharePoint Online, but the new unified approach is served from the Security and Compliance Center. The ability to create legal holds on SharePoint content within the SharePoint eDiscovery Center has been deprecated in 2017, and while the same deprecation was announced for legal holds in Exchange Online, these will remain on offer until late 2017 or early 2018 when those too will stop working in favor of a unified approach in the Security and Compliance Center. The current In-Place Hold in Exchange Online enables the creation of multiple separate legal holds that are transparent to the user, and that can be based on different parameters such as time-based, search query-based, and indefinite (until further notice).

Journaling is supported differently in Exchange Online versus Exchange Server; in the latter, an Exchange Server mailbox can be designated a journal destination, but in Exchange Online it cannot be. Microsoft supports some level of journaling in Exchange Online to non-Exchange Online destinations, but a) allows only a maximum of 10 journal rules to be created for an entire tenant, and b) would prefer the use of Exchange Online Archiving, not journaling.

We see the following weaknesses with the litigation-hold capabilities in Office 365:

- Current legal holds created in Exchange or SharePoint cannot be migrated into the new experience in the Security and Compliance Center. They are separate objects that must run their course and then expire, rather than being something that can be pulled across for a unified view of current and outstanding legal holds.

- The litigation hold capabilities deal only with content in Office 365, but not content stored elsewhere. Organizations with significant data repositories outside of Office 365 – on-premises and in other cloud services – will require multiple disparate systems, creating a complex legal compliance minefield.

- While many holds can be applied to a mailbox, the maximum number of keywords in all query-based holds placed on a mailbox is 500. If there are more than 500 keywords, then all content in the mailbox is placed on hold (not just that content that matches the search criteria). All content is held until the total number of keywords is reduced to 500 or less. Moreover, a legal hold can apply only to 10,000 mailboxes, but only 1,000 mailboxes in Advanced eDiscovery. Should more mailboxes be required, multiple holds must be created. Moreover, it is worth noting that only one hold may be applied to each email, and so an email cannot be on hold for two cases/reasons.

- Office 365 does not support the use of journaling to an Exchange Online mailbox for capturing a copy of communications to be used as part of a data archiving approach. Journaling rules can be specified that journal internal only, external only, or both types of messages to a non-Exchange Online destination, but once journaled, such messages cannot be touched by Office 365's litigation hold capabilities. Each Office 365 tenant can specify a maximum of 10 journal rules.

- No workflow support for coordinating with data custodians across the organization that may have content that is responsive to the legal hold

Current legal holds created in Exchange or SharePoint cannot be migrated into the new experience in the Security and Compliance Center.

parameters. While these could be manually created and sent, no audit trail reporting would be created for subsequent review.

- Searches for responsive material are point-in-time, and do not automatically keep the result set up-to-date. Human intervention is required to re-run all current legal hold searches, and then apply a hold to new material.

- Office 365 can search and index a specific list of file types (see above). If non-supported file types are identified during a content search, they will be flagged for human review. Organizations with file types not on the supported list will face ongoing costs for document-by-document review to meet legal or regulatory requirements.

- After searching for content in Exchange Online, the search preview pane will display a maximum of 200 items for an In-Place eDiscovery Search, listing the mailboxes and items found. However, these items cannot be displayed in the search preview pane; they must be exported to a discovery mailbox for review. Better in-line support for previewing messages directly from the search pane is not available.

  Some consider that the search workflow in Office 365 is cumbersome, particularly for complex searches and searches must be re-run through a series of pages to add more criteria. For companies that are heavy users of search, this can be a significant problem and is not as efficient as some third-party archives that are purpose-built and have more advanced and intuitive interfaces, as well as better search performance, to support these activities.

- For content searches based on multiple keywords, the search results do not show which keyword triggered the inclusion of a specific item. The only way for an analyst to know which keyword was responsible in Office 365 is to set up multiple, single keyword searches.

DATA RESIDENCY

Each Office 365 tenant has one and only one regional location, even for multi-national and cross-regional organizations with significant business operations in multiple regions. The master location of the tenant is selected when the tenant is initially provisioned, and this dictates where the organization's data is stored, which raises concerns from a data residency and sovereignty perspective. And some content types in Office 365, such as Yammer, are served only out of the North American region, regardless of the customer's master region. However, recent announcements indicate upcoming options for regionalization of Yammer.

An organization with significant operations in Europe and the United States, for example, cannot geo-ring fence content from its European operations to reside in a European Office 365 data center and also have the North American content reside in a North American Office 365 data center. The question of legal jurisdiction therefore becomes paramount in the case of a legal dispute or court order for access to data, and also more generally for protected data types that are required to remain in certain geographical areas, such as personal data under the EU's General Data Protection Regulation.

There are a couple of possibilities for forcing a multi-regional solution to issues of data residency and legal jurisdiction, such as building separate customer-controlled data centers in the different regions (thereby enabling geo-ring fencing of some content), or alternatively setting up and maintaining multiple, interrelated Office 365 tenants (which is a non-trivial undertaking that comes with significant technical requirements and less-than-ideal functional consequences). A new possibility from Microsoft is Multi-Geo Capabilities, announced at Ignite in late September 2017, and in private preview ahead of its launch in 2018. Multi-Geo will initially apply to Exchange, OneDrive and SharePoint in Office 365, and allows a single tenant to have users homed in different geographical regions.

Multi-Geo support is not free; it remains to be seen if the technical realities meet the promised capabilities, and equally if the pricing structure works for organizations that require multi-geo data residency.

eDISCOVERY WORKFLOW

Office 365 provides a range of eDiscovery capabilities to support search for responsive material, plus Advanced eDiscovery that adds text analytics, machine learning, and relevance and predictive coding to support early case assessment. The latter is available in the premium Enterprise E5 plan, and as an additional cost add-on to the Enterprise E3 plan. With its latest approach to eDiscovery through the Security and Compliance Center, Microsoft has finally removed some of the limitations from its earlier attempts to provide enterprise-class eDiscovery, such as limited search scopes (where a maximum of 10,000 Exchange mailboxes could be searched at once in an eDiscovery search), as well as separate eDiscovery tools for Exchange Online and SharePoint Online.

However, none of the eDiscovery tools in Office 365 provide a coherent eDiscovery workflow process for the modern organization. For instance:

- There is no workflow or project tracking of an eDiscovery case, such as the status of the case, who is involved, and which tasks are being worked on by whom.

- All cases are created and managed in an ad-hoc way, with a compliance officer entering ad-hoc search terms. It is not possible to create a case template for repeatability and auditing, with standard search queries and locations, key actions and requirements to complete, and an audit trail of what was and wasn't done. This is of particular concern to organizations that are not doing eDiscovery all the time; the ad-hoc approach means that prior learnings and approaches are likely to be forgotten and overlooked in a current eDiscovery case, potentially exposing an organization to sanction for insufficient production of evidence.

- The eDiscovery capabilities in the Security and Compliance Center take a unified approach to responsive content in three key Office 365 workloads: Exchange Online, SharePoint Online and OneDrive. However, an eDiscovery case created in the Security and Compliance Center cannot search for responsive content in non-Office 365 content repositories, such as those maintained on-premises or in other cloud services. This Office 365-only-and-nothing-else approach means that any organization with content outside of Office 365 will need multiple eDiscovery tools, in addition to having to instantiate, perform, and coordinate multiple eDiscovery cases in each separate tool. This is an expensive, complex, and error-prone situation.

- Search results for Exchange Online, SharePoint Online and OneDrive must be exported from Office 365 to facilitate the review process; the Exchange content as one or more .PST files, and the SharePoint and OneDrive content as individual files (with an option for all versions). There are multiple problems with the Office 365 approach: it creates a duplicate set of content outside of Office 365 which must be protected, there is no reporting on actions taken on the exported content in the eDiscovery case in Office 365 because Office 365 is blind to post-export actions, if the search is run again in Office 365 then a subsequent export is required along with integration of multiple sets of data, and there is no connection between what was collected and the coding decisions made to that content in order to inform future cases and reduce the volume of potentially responsive content in Office 365. The need to export content to Azure – with the time delays that introduces from Office 365 to Azure and then Azure to a local computer – introduces unhelpful delays in an urgent process for compliance officers.

None of the eDiscovery tools in Office 365 provide a coherent eDiscovery workflow process for the modern organization.

At Ignite 2017, Microsoft announced a new capability for customers with Advanced eDiscovery: import of non-Office 365 data into a specifically assigned Azure

container, which can be analyzed using Advanced eDiscovery. This requires an Advanced eDiscovery license for every user whose data is being analyzed, and later in 2017, a separate eDiscovery Storage plan, as well (500 gigabytes is $100 per month).

STORAGE OF AUDIT REPORTS

Office 365 offers a unified audit logging service across key workloads, and is accessed through the Security and Compliance Center. Auditing for most workloads is turned off by default (and thus must be turned on to start the process of collecting audit entries); one prominent exception is audit logging of administrator actions in Exchange Online, which is turned on by default. Audit entries in the Security and Compliance Center are retained for 90 days, after which they are purged. A recent change to audit logging of Exchange items means that an administrator can set a higher (or lower) default period. Advanced Security Management – an integrated component of the Enterprise E5 license and an optional add-on for other plans – captures audit log data from Office 365 and moves it to Azure, but even then, such audit log entries are stored for only 180 days (six months). Organizations that need long-term access to audit report items – such as seven years worth of data under some compliance regulations – should be aware of the limitations of the Office 365 Audit Log service, namely:

- Audit log entries are purged after 90 days, except for Exchange Online audit items if an administrator has specified a longer retention duration.

- Querying the audit log system in Office 365 allows a maximum query period of 90 days and cannot be changed.

- Exporting audit log items from Office 365 is limited to 1,000 entries unless all results are exported, for which the limit is 50,000 items. An organization with auditing turned on will generate at least 10-20 audit items per individual per day for a light user, and potentially a couple of hundred items per day for an active user. Some mid-sized organizations and larger organization will hit the 50,000-item limit every day. Consequently, an administrator will need to specify and generate at least one export every day, hoping that the time delay in capturing audit report entries does not result in an incomplete report.

- Exports are delivered as .CSV files, the collection of which must be managed. Paradoxically, as an exported file of audit items, there is nothing to prevent an errant administrator from removing evidence of their own wrongdoing; the exported file does not guarantee authenticity of the historical information purportedly contained inside, negating any chain-of-custody.

While Microsoft has increased its capabilities for the storage of audit reports over the past year, their handling still feels like a half-hearted attempt to meet a tick box requirement rather than delivering to the real business requirements of compliance reporting.

LICENSE REQUIRED FOR EX-EMPLOYEES' MAILBOXES

When an employee leaves the organization, but their mailbox must be retained, it was historically true that a full user license was still required to keep the mailbox. Microsoft has removed this licensing requirement, and so-called "inactive mailboxes" in Exchange Online can be retained free of charge. This means that an administrator can put a mailbox on legal hold and delete the associated user account; the mailbox is retained for the duration of the legal hold as an inactive mailbox without incurring any charge to the organization. However, Microsoft has signaled its intent to introduce a new license requirement for inactive mailboxes, originally scheduled to come into force from October 1, 2017, but for the time being has delayed the introduction of this cost. It is highly likely that inactive mailboxes will have new licensing requirement in the next 12-24 months.

DATA PROTECTION

Microsoft does not offer traditional backup and recovery capabilities for Office 365 as organizations have deployed in on-premises environments in the past. Instead, Microsoft uses different approaches for safeguarding current production data. Office 365 is a live production system that offers recovery of messages and documents within a rolling time window. In Exchange Online, for example, a user can recover a deleted item for up to 14 days (by default, although an administrator can increase the recovery window to a maximum of 30 days). A different option is to use litigation hold or an indefinite legal hold to prevent any mailbox item from actually being deleted. It will become hidden from the user's view when deleted, but it's still there in the mailbox. In SharePoint Online, there is also the ability to retrieve a deleted file within 30 days of deletion.

Microsoft does not offer point-in-time backup and recovery for organizations that want more traditional backup capabilities, and cannot retrieve items that have been deleted beyond their recovery timeframe (assuming the mailbox is not on litigation or legal hold.) Other disaster-level scenarios are also not covered by Microsoft's service offering.

SECURITY LIMITATIONS

In this section we investigate the gaps in Office 365 from a security perspective.

LIMITED DATA LOSS PREVENTION CAPABILITIES

The Security and Compliance Center in Office 365 offers a unified DLP policy creation and reporting engine for Exchange Online, SharePoint Online, and OneDrive for Business (but not other workloads in Office 365). In addition to these new unified capabilities, administrators are still able to create Exchange-only policies through the Exchange Admin Center. DLP policies include basic detection capabilities, for identifying keywords and regular expressions in an email or attachment. A regular expression, called a "regex" for short, is a way of representing a particular numerical or alphanumerical pattern for recognizing data such as a credit card or bank account number. DLP policies can stop and block messages that contravene policy, but lack more nuanced or advanced capabilities. We see the following shortcomings (and, potentially, many false positives) with the new DLP capabilities in the Security and Compliance Center:

- Exchange Transport Rules can look for sensitive data inside email messages and attachments (subject to the attachment being one of the supported file types). If the rule is triggered, there is no identification or classification of the sensitive data that caused the rule to trigger. The sensitive word, phrase or document property is not identified.

- The DLP capabilities in Office 365 apply only to Exchange Online, SharePoint Online, and OneDrive for Business. Organizations with other content storage and routing systems will require separate DLP capabilities. The Office 365 DLP solution does not provide a unified DLP rules and remediation engine that covers Office 365 and other services being used by the organization.

- A DLP rule cannot specify a data redaction action, where sensitive data in a message is removed (and highlighted as being removed) while flowing the rest of the message to the intended recipient. If such data is identified, the message can be blocked or escalated for approval; redaction is not an option either as an automated action or as an approval action by the designated moderator. This creates additional work for a compliance officer or IT administrator, while still potentially allowing a sensitive credit card or bank account number to be sent through the system.

Microsoft does not offer point-in-time backup and recovery for organizations that want more traditional backup capabilities.

- A DLP rule cannot remove sensitive or protected information from messages and documents, nor scrub out document properties or metadata attributes that should not be sent to other people. Messages with such information – if detected – can be blocked or flagged for review, but not automatically cleansed and sent on for delivery.

- A DLP rule can forward a violating message for approval to an explicitly named individual or the sender's manager. There are no additional options for directory lookups based on the sender's name, such as the compliance officer for the sender's department, or the sender's manager's manager.

- Multiple conditions within a DLP rule can have only the AND operator between them. There is no support for the more nuanced OR, or a combination of AND and OR conditions within a single rule. For example, to capture an attachment that contains the phrase "Top Secret" and/or has a specified document property set to "Top Secret" requires two separate rules. The first rule will capture the attachment if the phrase is included, and the second if the property is set. This means administrators will have to develop, test and deploy potentially hundreds of rules with slightly different conditions and the same actions so as to capture the variations in use. And it is impossible to know whether a rule set is effective or not, because there is no alerting on near-matches based on a confidence level, fuzzy logic, or machine intelligence.

- New or modified rules are not enabled in real-time; a delay of several hours is common before they start working. This makes it very difficult for an administrator to test and verify the efficacy of a new or modified rule. Indeed, messages that should be triggered by the rule still flow through unhindered, and the administrator is blind to anything that is not explicitly captured (the threat level is unknown). Office 365 also does not offer a rule simulator with, for example, a curated set of 100 test messages and attachments that should trigger new or modified rules.

- Messages routed for approval can be approved only in Outlook on Windows and the Outlook Web App. The approve and reject options are not available in Outlook on Mac, nor Outlook on mobile devices, and there are no directions provided to jump to a Web interface to approve or reject the message.

- The DLP rules are blind to file types not supported on Office 365 – the list of 58 that is weighted in favor of Microsoft Office. This means that if non-supported file types are sent through Exchange Online that any DLP rules looking for phrases or properties in attachments will not be captured; the rule will not be triggered.

LIMITATIONS ON IDENTIFYING AND BLOCKING EMAIL FRAUD

CEO Fraud, Business Email Compromise and whaling (collectively, "BEC") is a growing problem and has cost organizations hundreds of millions of dollars over the past few years. While Office 365 attempts to block BEC using basic filtering, policies and authentication, these are not an effective method of preventing BEC attacks, exposing users to the variety of techniques that attackers use to evade detection. For example:

- Using a spoofed display name and sending the email from a known good domain, such as gmail.com, can ensure that domain reputation and basic authentication can allow a message to get through security defenses, increasing the likelihood of the attack being successful.

- Using a lookalike domain is another effective technique to trick victims. The most common method of creating a lookalike domain is to switch out a single

character, such as substituting a lower case "I" for a lower case "L", as in "tefion.com" instead of "teflon.com".

Because of the numerous ways that an attacker can use, this malware-free method of attempting to bypass security defenses can render the native capabilities in Office 365 relatively ineffective at stopping them.

LIMITATIONS ON ACCESS TO THE SPAM QUARANTINE

The default action in Office 365 is to deliver suspected spam to each user's junk mail folder, giving each person full access to their spam backlog. With the resurgence of spam over the past year being used to carry ever-emergent ransomware threats, this is a dangerous approach. The option is to turn on the spam quarantine for the organization – which requires Web browser access along with a username and password – to enforce an additional set of steps for end users wanting to check their quarantined messages and thus reduce the likelihood of spam-borne threats from being activated. Microsoft's implementation of the spam quarantine in Office 365 suffers from the following weaknesses:

- A maximum of 500 messages are displayed in the spam quarantine; there is no ability to view more. An end user can attempt to filter their list of spam messages to find the valid business emails inadvertently captured as spam, but the interface and message limit does not make this an easy process. It is more likely that valid messages that have been labeled as spam will remain undetected.

- Quarantined messages are retained for a maximum of 15 days, after which they are deleted and not retrievable. An administrator can decrease but not increase this number. If a valid business email is incorrectly labeled as spam and the end user does not review his or her quarantine for more than 15 days, those messages will be irretrievably lost.

Quarantined messages are retained for a maximum of 15 days, after which they are deleted and not retrievable.

ADVANCED THREAT PROTECTION

Customers paying for the most expensive Enterprise E5 plan – or those paying additional for the optional Advanced Threat Protection (ATP) add-on – get advanced protection from threats in name only. ATP offers two advanced capabilities: Safe Attachments and Safe Links. The first is supposed to capture and neutralize threats in attachments on inbound email messages, and the second is supposed to prevent malicious links in email messages from triggering an active threat. The problems with both capabilities are numerous, including:

- The two ATP services work only against inbound email messages and attachments. They are not activated for outbound or internal email, and are therefore unable to provide any protection or remediation for compromised Office 365 accounts.

- The ATP service delays email processing and routing. The Safe Attachments service can add 10-15 minutes for testing for vulnerabilities, with some customers reporting up to 30 minutes for a message, and three to five hours at peak times.

- Unsafe attachments have previously been treated as safe by the Safe Attachments service. The service has been ineffective at identifying new and emergent malware threats, and various ways of getting around the protections in Safe Attachments have been documented, such as by using large files, zipping a file twice, obfuscating the injection of macros, delivering zero-kilobyte file attachments that trigger malware, and locally-produced files that conceal malicious coding, among others. Microsoft is in a constant cat-and-mouse game trying to fight off actors with malicious intent. There have also been recent reports that compromised files stored in SharePoint Online and OneDrive for

Business – trusted storage locations for Microsoft – have slipped through the Safe Attachments service.

- The Safe Links service has been shown to allow through unsafe links, the consequence of malicious actors figuring out how to circumvent Microsoft's protections. One recent example has been exploiting the Punycode limitation to trick the malicious link checker with the safe ASCII version, while then using the Unicode version of the link to direct the browser to a malicious site.

- The Safe Links capability does not actually analyze the destination site to see if it contains any threats; it merely checks the link against a blacklist. If the site is not on the blacklist, the user is passed through to the destination.

- Up until late September 2017, the Safe Links service rewrote the original URL in the message with a "safe" version that had to be processed by Office 365 each time it was clicked. The safe version obfuscated the original, removing the possibility for the end user to check the validity of the link, for example, that the text link in the message matches the underlying destination presented when hovering over the link. However, announced at Ignite 2017 is that URL wrapping has been removed from links and users can now hover over a link to see the original URL.

- Safe Links scans only URLs in email messages and attachments opened in Office ProPlus on Windows. URL links in other types of attachments are not passed through the Safe Links service, nor on other versions of Office or Office installed on non-Windows devices.

- At Ignite 2017, Microsoft announced that Safe Links now also protect internal emails to protect against compromised accounts. Also announced was a new capability that enables a user to preview the content of the attachment even as it is being scanned; the user can interact with the preview document as they would with the real document, e.g., making edits or other changes. (What we do not know as of this writing is whether or not these edits and changes are automatically integrated into the delivered document.) Also at Ignite 2017, Microsoft announced that ATP now supports additional Office 365 workloads, such as SharePoint Online, OneDrive for Business and Microsoft Teams.

- Microsoft has also announced that Safe Links will be available for Office clients on the iOS and Android platforms before the end of 2017, but this will be only for supported file types (i.e., not for non-Office attachments). Moreover, detonation is now available to detect phishing URLs in the email body and within attachments, but again, only for supported file types.

In light of the above realities, it is fair to say that Microsoft's Advanced Threat Protection in Office 365 is better than no "advanced" protection, but insufficient compared with the active threats it is supposed to protect against.

LIMITED THREAT PROTECTION FOR INTERNAL ACTIVITY

Multi-stage attacks and fraud schemes use phishing emails internal to organization from compromised devices or email accounts. The threat protection capabilities in Office 365 are focused on mitigating incoming threats and provide little protection for the threats that flow inside the organization or from inside to outside. Internal email is not routed through Exchange Online Protection nor Advanced Threat Protection (if licensed). However, Microsoft has recently announced that Safe Links now also protects internal emails to defend against compromised accounts.

NO UNIFIED VISIBILITY ACROSS THREAT VECTORS

The threat reports in the Security and Compliance Center focus on malware and spam, but ignore other non-malware based attacks, including credential phishing and email fraud. The lack of unified visibility into all types of threats makes it extremely

difficult to see the big picture: what is happening, how are the threats morphing, and what are the current threat vectors that need additional protection.

LIMITED ABILITY TO ENABLE COMPLEMENTARY, RATHER THAN REPLACEMENT, SECURITY SERVICES

In light of the general and specific weaknesses in the security capabilities of Office 365, customers can benefit from additional assurance and true advanced mitigation capabilities provided by specialist third-party security solutions. The ideal for adding layers of security is a collaborative multi-layer approach, whereby additional layers process incoming threats before handing the message to Office 365. Each message can then be processed by Office 365 for its own security testing and assurance, and likewise protect internal plus outbound messages with additional, complementary layers of security.

There have been cases, however, where adding layers of security before Office 365 has resulted in the Office 365 security services no longer working; the new front-end security capabilities are treated as trusted delivery mechanisms that render Office 365's own security ineffective. In the rapidly evolving threat landscape in which organizations find themselves, Microsoft needs to offer better possibilities for third-party security vendors to deliver complementary, rather than replacement, security services.

AUTHENTICATION

Authentication to Office 365 is managed through Azure Active Directory (Azure AD), a cloud-tailored version of Microsoft Active Directory. All users must sign in with a username and password. For added security, Microsoft offers multi-factor authentication using SMS one-time passwords, the Mobile Authenticator app, and phone verification. Microsoft offers various ways for integrating an on-premises directory (such as Active Directory) with Azure AD and third party identity providers, in order to simplify the user authentication process for end users.

It is vital to get user authentication right given the sensitive information stored in Office 365 accounts, and many security professionals question the general reliance on usernames and passwords, and lighter forms of multi-factor authentication. We see the following shortcomings in the authentication approaches offered by Microsoft:

- **Limited support for common single sign-on protocols**
  Single sign-on (SSO) requires the use of an authentication protocol, of which there are many. Microsoft can interoperate with a number of third party SSO Identity Providers through OIDC, SAML 2.0, WS-Federation, and WS-Trust protocols. Because some O365 rich clients use legacy authentication, while others are capable of modern authentication, customers must select an Identity Provider capable of handling all of their authentication needs.

- **Limited support for third-party hardware authentication tokens**
  Azure AD provides identity management for Office 365 and can be integrated with other directory services in various (and frequently changing) ways. However, with only a few exceptions (e.g., RSA SecurID Access), Office 365 does not support the variety of third-party hardware-based authentication tokens available on the market, such as YubiKey and other one-time password devices. YubiKey, for example, enables users to sign-in to computers, mobile phones and cloud service accounts without having to enter a password; the presence of the hardware authentication token removes the need for entering a password. These offer a more secure second factor for authentication than using SMS-based and app-based approaches because there is no network traffic required (which could be subject to eavesdropping), can eliminate social engineering attempts by an attacker to get a replacement SIM card, and can verify domain and app validity to reduce phishing threats. Customers interested in leveraging Multi-Factor Authentication (MFA) along with O365 rich clients must ensure that they are using clients capable of performing "modern authentication."

It is vital to get user authent-ication right given the sensitive information stored in Office 365 accounts.

- **Lack of support for extensively branding the login page**
  Third-party solutions that permit customized branding of the Office 365 login page provide better protection against phishing attempts than the standard login screen available with Office 365. Customized branding assures users that if they accidentally or even deliberately click on a link contained within the phishing email and don't see the expected, corporate branding, it's likely to be a fake Office 365 login screen. Since hacker solicitations are fairly common using the standard Office 365 login, customized branding provides an additional layer of defense against phishing attempts.

- **No support for universal single logout**
  Office 365 does not offer the ability to terminate all SSO-based sessions with a single action. There is no "logout everywhere" option for users so they can be assured that no active sessions are retained. Such an approach is essential for ensuring only valid logins are active, and can be used to check that the user's credentials are still secure (and have not been compromised).

- **No support for passphrases**
  Recommendations for creating strong passwords have focused on increasing their length (more than 10 characters) and their complexity (mixed lower and uppercase alpha characters, plus at least one numeric digit, and maybe a non-alphanumeric character such as @ or ^ as well). With added length and complexity comes a greater likelihood of the user forgetting their password, and with people using many services that each need a username and password, the likelihood of using the same password across many services increases. Passphrases are a strategy to replace passwords altogether, using a short phrase in place of a complex password. For example, the passphrase "I went to school in New York in 1986" is easy to remember, but extremely difficult to crack due to its length. Office 365/Azure AD does not support the use of passphrases, however, because passwords cannot contain spaces, and can be no longer than 16 characters. NIST's latest recommendation for passphrase length is at least 64 characters, a significant increase over what is offered in Azure AD.

- **Lack of context-aware authentication**
  Office 365 does not include step-up authentication, which requires a user to authenticate at a level based on a pre-established policy for a particular resource. This context-aware authentication can be based on a user's geolocation, the access points from which they are accessing the resource, or whitelisting/blacklisting by the user, group or organization.

- **Other limitations**
  Unlike some other authentication solutions, Office 365 does not provide the ability to provide extensive or customized authentication reporting for compliance and fraud detection, nor does it provide more flexible password-recovery capabilities.

OTHER ISSUES

We have looked at the major limitations in Office 365 in the areas of archiving, compliance, security, and authentication. Beyond these major areas, there are a few other limitations in Office 365 to consider:

CANNOT TAILOR ADMINISTRATOR TYPES

Microsoft offers a range of administrator types for Office 365, but does not provide the ability to tailor these for organizations with multiple businesses within a single tenant. For example, an organization cannot use role-based access control to divide administration responsibilities for Azure AD across multiple domains in a single tenant.

LACK OF INTEGRATION WITH THE BROADER ECOSYSTEM

While the security capabilities in Office 365 integrate quite nicely with other security offerings, most of these integrations are between Microsoft offerings, not between those that are not offered by Microsoft. Third party tools provide these needed integrations to ensure that an organization's entire security ecosystem can be properly managed.

LACK OF EMAIL CONTINUITY

Email has become such an integral part of the way that people work that email disruptions of even 15 minutes can have significant impacts on user productivity. The lack of native email continuity capabilities in Office 365 can have significant impacts on user productivity, although there are third party solutions available that will provide both disaster recovery and business continuity capabilities to ensure that users have access to email and other capabilities.

SUMMARY

We have reviewed the current capabilities of Office 365 in the areas of data protection, archiving, security, encryption and eDiscovery, among others. Microsoft offers a wide range of capabilities in these areas, but nonetheless, we have explored multiple areas of significant concern with the capabilities that are on offer.

In summary, we say:

- **Keep using Office 365**
  It offers tremendous value to organizations, is highly strategic to Microsoft's current and future revenue streams, and is continually being improved.

- **Don't put all your eggs in one basket**
  While Office 365 offers many good capabilities in the areas we have explored, customers are likely to experience limitations that can be mitigated by best-in-class third-party vendors.

- **View third-party integrations as strategic, not tactical**
  While Microsoft will keep improving Office 365, specialist third-party vendors will continue to offer best-in-class capabilities to protect and provide assurance for the modern organization.

SPONSOR OF THIS WHITE PAPER

Viewpointe helps to address information challenges and automate content processes with OnPointe, a suite of content service solutions that help improve information management and document processes across the enterprise with the flexibility to focus on current content challenges while also providing a foundation to address future business needs. Viewpointe has the expertise to assist with professional services to guide implementation and project success, content services to meet functional requirements with system connectivity and embedded end-user interfaces and proven managed services in a private cloud environment to keep content secure. In addition, Viewpointe delivers the promise of flexible, future-proofed cloud services without sacrificing the security and compliance demands of regulated businesses.

Viewpointe allows you to take control of business content across a broad range of enterprise applications, messaging systems, content repositories and even file shares that often go unmanaged. Designed to handle petabytes of information, OnPointe provides specific services and integrations to ingest and classify many types of structured and unstructured information. With our extensive APIs, even custom or in-house developed applications can be integrated, helping to insure consistent governance of data.

www.viewpointe.com

@Viewpointellc

+1 800 956 3807

Five key capabilities comprise the OnPointe suite of private cloud-based content services include:

- Content capture and management
- Search, retrieval and version tracking
- Security and privacy controls
- Retention management and disposition
- Workflow automation of content processes

Viewpointe's cloud-based managed services help streamline the information lifecycle and automate business processes with a foundation of compliance and information governance. Known for its time-proven expertise in information strategies and managed services, Viewpointe makes it possible to address today's business opportunities and risks while planning for tomorrow's challenges. Founded in 2000, Viewpointe has been named to the prestigious FinTech 100, representing the best in financial technology and service providers every year since 2006 and is the chosen partner at many of the world's most esteemed companies.