Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **January 2019**
Sponsored by **Agari**

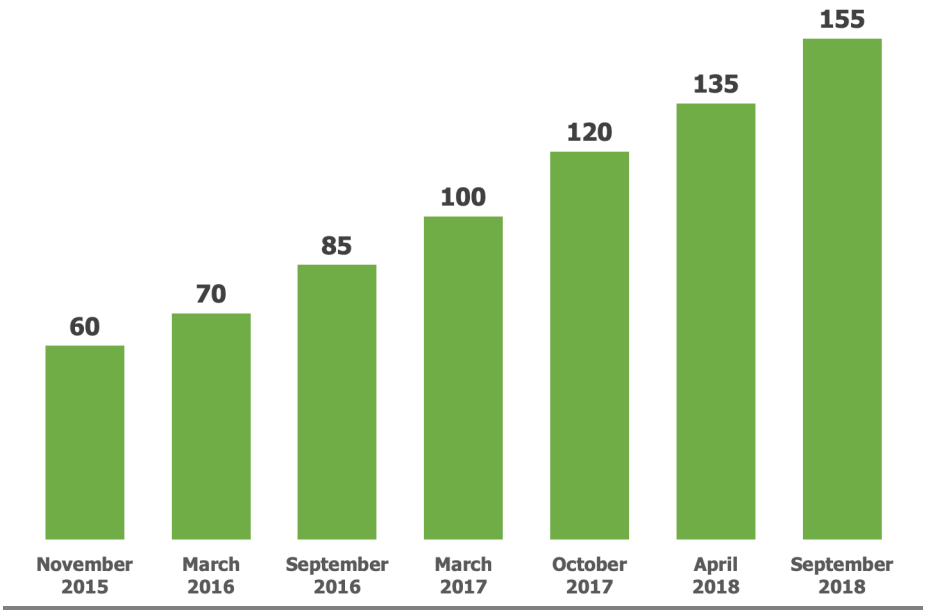
Why Your Company Needs Third-Party Solutions for Office 365

agari
by HelpSystems

Executive Summary

Office 365 is a capable and robust communications and collaboration platform. Microsoft has assembled a wide collection of features and functions that can satisfy a range of corporate requirements for email, voice, desktop productivity and collaboration that has proven to be highly successful, as demonstrated by the significant growth in users of the platform, as shown in Figure 1.

Figure 1
Microsoft Office 365 Subscriber Numbers in Commercial Organizations
Millions of subscribers



Source: Microsoft

Microsoft has assembled a wide collection of features and functions that can satisfy a range of corporate requirements for email, voice, desktop productivity and collaboration.

Microsoft is attempting to deliver a cloud service that does many things for a broad range across productivity, security, compliance, and data protection. This is a significant task and has many complexities and inter-dependencies that must be traded off against one another. Like any large platform with a large and diverse user base, it frequently provides a "good enough" capability in many areas, but does not necessarily provide the depth of capability or specialized solutions for customers with needs and requirements beyond the basics. These may be companies looking for deeper functionality or better performance in specific areas, or companies with specialized needs, like companies in regulated sectors or those subject to new multi-sector data protection legislation that need to satisfy their legal, regulatory or best practices requirements.

The tight inter-linkages between multiple services also create single points-of-failure, such as the two multi-factor authentication meltdowns that occurred during November 2018. Moreover, Osterman Research has found that many third-party solutions often present a better alternative to some of the native capabilities within the Office 365 platform.

In short, Osterman Research believes that Office 365 and Exchange Online are important and capable platforms that should seriously be considered for use by just about any organization. However, decision makers should understand their real requirements and identify any feature or performance gaps vis-à-vis the platform. Office 365 provides a solid foundation to which many organizations should then add third-party solutions in order to provide higher levels of security, content

management, encryption and other capabilities. We note that the use of third-party solutions will often enable the use of less expensive Office 365 plans, resulting in a total cost of ownership that can be lower than if more expensive Office 365 plans are used.

KEY TAKEAWAYS

- **Many organizations will implement third-party solutions**
  Our research found that nearly one-third of organizations that are implementing Office 365 have plans to use a combination of less expensive plans in conjunction with third-party solutions that will provide improved security, archiving or other capabilities than what is available natively in the Office 365 platform. In fact, 37 percent of the typical Office 365 budget in 2019 will be spent on third-party security, archiving and other solutions.

- **Email is the fundamental driver for Office 365**
  Not surprisingly, the vast majority (93 percent) of organizations consider email to be an important or extremely important capability in Office 365. By contrast, other Office 365 capabilities are not considered to be this important, including Skype for Business (54 percent), SharePoint Online (47 percent) and OneDrive for Business (45 percent).

- **Limitations for targeted and more advanced threats**
  Most organizations currently subscribed to Office 365 rely on the basic security offered natively in the platform. For those using a version with Microsoft's Advanced Threat Protection (ATP), it is a more capable security offering, but it does have some limitations, including the fact that not all content is actively scanned in place for embedded threats in SharePoint Online, OneDrive for Business and Microsoft Teams; and Scanning email attachments for unknown threats using ATP can delay delivery and impact user productivity. Office 365 subscribers interested in ATP should consider security options from specialized security providers.

- **Lack of a consolidated view of threats**
  The various threat reports in the Security & Compliance Center do not provide a consolidated view as would be available in some third-party security solutions.

- **Hybrid management must be considered**
  Many organizations are transitioning to hybrid environments in their eventual migration to Office 365 – our research finds that 13 percent of organizations plan to maintain a hybrid configuration for the long-term. Hybrid environments introduce additional, and sometimes unforeseen, management and administration complexities that, if not properly addressed with new processes and third-party tools, risk wiping out many of the benefits of the Office 365 implementation.

- **Some applications will exist only in the cloud**
  While users still working on-premises are enjoying more parity with what is available in the cloud, especially with the Office 2019 release[i], there are still some applications, such as Workplace Analytics[ii], that will be available only as a cloud service. Organizations that wish to take advantage of such solutions will require some form of integration.

- **Limitations for preventing impersonation**
  Impersonation through spoofed, lookalike and soundalike domains are a very serious issue in the context of phishing and spearphishing attempts. Office 365 will notify the recipient of a suspicious message that spoofs the organization's domain name, but the match must be exact – Office 365 does not deal with near matches due to similar domains that look or sound similar to the organization's domain.

...37 percent of the typical Office 365 budget in 2019 will be spent on third-party security, archiving and other solutions.

- **Limitations in data loss prevention (DLP)**
  DLP policies in Office 365 are evaluated in priority or execution order, and the first rule that matches identified content in an email message or document is applied. There is no ability to set the priority or execution order of DLP policies, apart from the sequence in time of creating them.

- **Problems with encryption capabilities**
  Microsoft's reliance on link-based messages for recipients without Outlook means that encrypted messages can look like phishing messages, especially since they then request a username and password to login. Since a common phishing vector is to use a faked Office 365 login screen, wary users may hold back from engaging with encrypted messages, or alternatively become desensitized to the threat of phishing and inadvertently open a phishing message and give away access to their credentials.

- **Limitations in eDiscovery**
  There is no workflow or project tracking of an eDiscovery case in Office 365, and searches for keywords that are started in the Content Search tool cannot be imported into an eDiscovery case.

- **A limited number of file types are indexed**
  When undertaking an eDiscovery search and performing an Early Case Assessment, any file that is not included in the 58 files types that Microsoft supports will be flagged as unprocessed.

- **No long-term storage of audit logs for compliance purposes**
  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 dictate retention of this data for much longer periods.

ABOUT THIS WHITE PAPER

This white paper was sponsored by Agari; information about the company is provided at the end of the paper. The paper includes data from an in-depth survey that Osterman Research conducted in October 2018. We surveyed 124 organizations with a median of 1,400 employees to understand the problems they face in managing Office 365, additional capabilities they would like to have, and other relevant information about their Office 365 environments. The data from the survey will be published in a separate survey report following publication of this white paper.

The paper includes data from an in-depth survey that Osterman Research conducted in October 2018.

Considerations for Office 365 Security

ACCESS TO THE SPAM QUARANTINE

There are a number of issues with regard to the Office 365 spam quarantine that decision makers should consider as they evaluate third-party solutions that might provide better security capabilities.

- Only 500 messages can be 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.

- An administrator cannot view all messages held in the quarantine in a single list. They must be divided into the different types of messages that are held in the quarantine, such as spam, malware, phishing, and bulk.

- Quarantined spam messages are retained for a maximum of 30 days (introduced September 2018), after which they are deleted and not retrievable. Microsoft says that the default duration is also 30 days, but a check of several tenants had the default still set at 15 days. An administrator can decrease, but not increase, this maximum 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 30 days, those messages will be irretrievably lost.

- It is not possible to create different policies to deal with different types of spam and bulk messages, such as spam, malware, phishing, and bulk matches. An anti-spam policy can be differentiated based on recipient, but not based on type of message.

- When adding an X-header within a policy, the X-header has to be the same for each type of spam or bulk message; there isn't an option to differentiate the X-header based on type (e.g., spam, malware, phishing, or bulk).

- While spam is only one category of message that might be quarantined, a single setting under anti-spam sets the quarantine period for all categories of messages that are quarantined; there is no option to set a different retention period based on different types of quarantined messages.

- For end users, there is no workflow for releasing spam from the quarantine. If a user wants a message put into their inbox, the action is executed directly. There is no possibility for flagging a message for release and enabling an administrator to check the message before the actual release action is triggered.

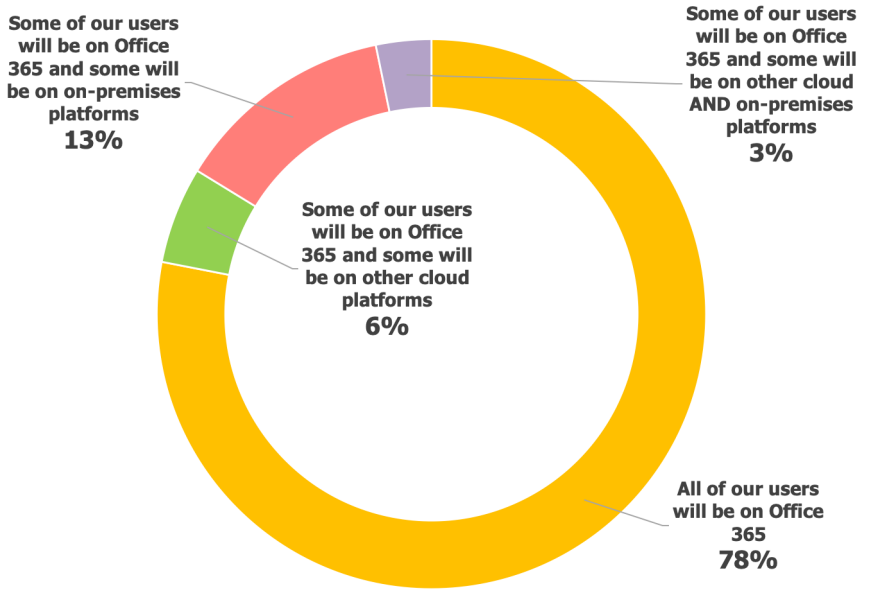
- Messages from blocked senders are still sent to the spam quarantine, rather than just being deleted immediately. This can overload the quarantine with possible spam, as well as email from blocked senders.

- The quarantine doesn't share intelligence with users on how many similar messages were received with a similar subject line and sender by other people in the organization. A higher number would signal the likelihood that the message is spam or a phishing attempt, but this intelligence is not offered to help users make informed decisions about the likelihood of a message carrying malicious intent.

- Microsoft's new Zero-hour Auto Purge (ZAP) feature does not support the spam quarantine. While it can automatically re-classify messages incorrectly classified as spam or mis-classified as clean, and move messages between the user's inbox and Junk Mail folders, it cannot move messages automatically between the spam quarantine and inbox. Plus, ZAP works only with Exchange Online inboxes, which presents a problem for organizations that maintain a hybrid environment. This is an important issue for organizations that are deploying Office 365 given the large number of other solutions that will co-exist with Office 365, as shown in Figure 2.

It is not possible to create different policies to deal with different types of spam and bulk messages.

Figure 2
Deployment Environments Once Office 365 is Fully Deployed



Source: Osterman Research, Inc.

- An administrator can turn on spam notifications for end users, which is a once-a-day email message listing messages in the quarantine addressed to the user which were classified as spam. However, it is important to note that:
    - The notification is for spam only. Other messages sent to the quarantine are excluded.
    - Notifications regarding spam messages held in the quarantine can be sent only to everyone or to no one. Office 365 does not have a fine-grained ability to specify which users should receive notifications, nor which users should not.
    - It is not possible to specify the time of day for delivering the spam notification message from the quarantine, nor how frequently it should happen below the unit of days (e.g., there is no possibility to request a notification message every few hours). When the spam notification is received in the middle of the night, users could miss the notification.
    - While messages can be released from the quarantine from the notification message, each one must be handled in turn, necessitating yet another new browser window for each message the user wants to release to his or her inbox.
    - The notification message lists quarantined messages using Universal Coordinated Time (UTC) for all users. It pays no attention to the date/time zone settings for the user, thus displaying messages in a technically-correct but user-irrelevant format.
    - It is not possible to generate a spam notification message as soon as a new spam message is received. Notifications are sent daily, and not more frequently.

While messages can be released from the quarantine from the notification message, each one must be handled in turn.

TARGETED AND MORE ADVANCED THREATS

Advanced Threat Protection (ATP), a security service offered in Office 365 Plan E5 (or available as a standalone service), offers protection against advanced threats hidden in URLs, phishing messages, and documents. For the added cost of ATP, the service has some issues to consider. While organizations that meet some use cases may get better protection from ATP than from the standard Office 365 service, the risk landscape means that organizations would be well advised to consider third-party offerings that provide more advanced protection. In fact, we've come across organizations with Office 365 ATP that have also added an additional layer of security on top of that. Issues to consider include:

- ATP offers the possibility of checking attachments and links for unknown and emerging threats, but before it can do so, an administrator must set up policies to apply Safe Attachments and Safe Links to individuals, groups and the organization. No threat protection is on by default, and even when it is on, users must be connected to Office 365 in order for Safe Links and Safe Attachments to work.

- While ATP newly supports content at rest in SharePoint Online, OneDrive for Business and Microsoft Teams, not all content is actively scanned in place for embedded threats. Files are scanned based only on various selection criteria, such as sharing activities, guest access, and other threat signals. ATP cannot provide a real-time dashboard of malicious files in Office 365. Additionally, many organizations store content in other SaaS applications, such as Box or G-Suite, which are not covered by ATP.

- Scanning email attachments for unknown threats using ATP can delay delivery and impact user productivity. When ATP was first released, some customers complained that emails were being delayed by 10 to 15 minutes on average, and up to three to five hours at peak times. In late 2017, Microsoft claimed that its average latency was around 60 seconds, but some customers continue to complain into 2018 that the average processing time they experience is unacceptable. Microsoft has introduced various countermeasures to reduce the perception of delay, including Dynamic Delivery and Document Preview, the latter of which enables the user to view and edit a safe version of the document while the full document is still being scanned. It remains to be seen how long these safe versions delivered via Document Preview remain safe, as threat actors work actively to circumvent the new controls.

- Safe Links will check a URL at time-of-click against known blacklists of malicious sites. It does not actually evaluate for the presence of threats at the destination URL at time-of-click. Safe Links will pass a user through to a malicious web site if that site is not on a blacklist of known malicious sites. Some third-party solutions offer dynamic URL scanning to check suspicious URLs before the time-of-click.

- Safe Links evaluates URLs at time-of-click, but once a link is evaluated as malicious when a user clicks it there is no ability for Advanced Threat Protection to remove instances of the same email from other users' mailboxes.

- Microsoft is partially adding detonation to its URL checking repertoire through an integration with Safe Attachments. Documents linked via a URL in an email or document will now be detonated at time-of-click in Safe Attachments (for supported file types – such as Word, Excel and PowerPoint – and PDF documents as well). Sometime in the future Microsoft expects to use actual detonation for all URLs, although this is not yet available. Other, best-in-class solutions offer full URL detonation, which can detect malware-free attacks, such as credential phishing.

- Safe Links is designed primarily with users of Word, Excel and PowerPoint in mind, as long as they are using the Office 365 ProPlus versions on Windows or iOS and Android devices and are signed into the Office 365 service. It does not

We've come across organizations with Office 365 ATP that have also added an additional layer of security on top of that.

check links in other file formats or when the user is on a Mac. And, as noted above, the link is checked only against controlled blacklists rather than actually checking to see if the link is currently safe for the end user.

- 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. In our estimation, Microsoft's ATP is not quite as good some best-in-class, advanced, third-party offerings on the market.

- Safe Links has previously been tricked into approving malicious links for end users. For example, the Punycode limitation has been exploited to deceive 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. Malicious actors are constantly evaluating how to evade Microsoft's controls.

- Neither Safe Attachments or Safe Links are effective against CEO Fraud/Business Email Compromise (BEC) messages that typically contain no dangerous link and no attachment. Some third-party solutions offer dedicated protection for these threats, including protection against homograph domain attacks.

- Customers cannot monitor the status of ATP within Office 365; its service health is bundled with other services. This means that customers paying the additional cost for the service cannot know if the service is currently impacted by an outage or other degradation, or is just being non-performant.

- ATP lacks hybrid capabilities, meaning that customers with Exchange or SharePoint on-premises, for example, must have a second and separate threat-protection offering. ATP handles only certain Office 365 workloads under specific conditions, and does not address data and systems beyond Office 365. This can cause problems with many customers operating a hybrid environment.

- Microsoft says that ATP and Exchange Online Protection (EOP) together identify only 600 million emails out of 400 billion emails each month as being malicious; this is a malicious catch rate of 0.15 percent. This is significantly lower than the 0.99 percent malicious email rate identified by FireEye, for example[iii].

DATA LOSS PREVENTION CAPABILITIES

Office 365 offers two data loss prevention (DLP) engines: the older, established approach that carried across from Exchange Server on-premises, and the newer, unified approach through the Security & Compliance Center. Both offer DLP capabilities, but suffer from a number of weaknesses.

Office 365 offers two data loss prevention (DLP) engines.

DLP in Exchange Online:

- DLP rules support only basic actions when sensitive information is identified, lacking some of the capabilities of competitive offerings. For example, while DLP rules can stop a message and some types of documents from flowing through Exchange Online when sensitive information is identified, it is not possible to redact or sanitize the sensitive information in the message or document, or automatically encrypt when required, and still flow the message through to the recipient. Human intervention by the original sender or an administrator is required to fix the identified problem, which can create a backlog of messages requiring manual assessment and intervention to resolve.

- Basic document fingerprinting is available, where a template of a sensitive document can be saved and used for identifying future documents that have the same structure. Only full matches to the specific document fingerprint will be identified, however, while partial matches will evade detection.

- A message that violates a DLP rule can be routed only for review or approval to an explicitly named individual or the sender's manager. There are no more nuanced options, such as performing a directory lookup based on the sender's name or department name to find the local compliance officer, or routing messages to a quarantine for analysis by a group of administrators.

- DLP rules will detect sensitive information only in a specific set of 58 file types, which are weighted in favor of the different variants of Word, Excel, PowerPoint, and other Office file formats. Non-supported file types containing sensitive information will not be captured if they are sent through Exchange Online. Likewise, sensitive information hidden in images will not be identified because Office 365 cannot perform OCR on scanned documents and screenshots.

DLP in Office 365 Security & Compliance Center is the newer, still maturing approach that works across several Office 365 workloads (but not all of them), and is outstripping the capabilities of the Exchange Online approach. Issues for customers to consider include:

- DLP policies cannot proactively flag email sending mistakes, such as addressing an email to the wrong recipient due to auto-complete errors. Office 365 does not analyze a user's normal sending patterns to warn of misaddressed messages, and lacks advanced anomaly detection capabilities to detect malicious intent in email sending behavior.

- DLP policies are evaluated in priority or execution order, and the first rule that matches identified content in an email message or document is applied. There is no ability to set the priority or execution order of DLP policies, apart from the sequence in time of creating these. When a new policy is created, it is added at the end of the priority or execution order. By implication, to elevate the execution order of a new DLP policy, current policies would need to be deleted and re-created after creating the new DLP policy. This will undoubtedly introduce errors.

- There is no balanced analysis of which DLP policy would be best to apply to a specific message or document, or no attempt at identifying the "best match" on a message-by-message or document-by-document basis. In other words, a general policy that has a higher priority or execution order will be applied ahead of a specific policy that has a lower priority or execution order.

- There are no workflow options for messages and files that violate a DLP policy. For example, if an email message triggers a policy, it is either blocked or encrypted. There is no policy action option for routing the violating message to an administrator or administration queue for review. As with DLP in Exchange Online, DLP in the Security & Compliance Center doesn't offer any nuanced options to request a review by someone other than the original end user.

- While Office 365 offers DLP capabilities, these are limited to Exchange Online, SharePoint Online, and OneDrive for Business. The newer conversation tools in Office 365, such as Yammer and Microsoft Teams, are excluded, as are other document storage and conversational systems outside of Office 365. This partial coverage of Office 365 workloads means that Office 365 does not offer a unified DLP rules and remediation engine that can be used for all document storage and conversational systems in use across the enterprise, nor does it handle everything in Office 365. Microsoft has promised the ability to block chat messages in Microsoft Teams before the end of March 2019.

DLP policies cannot proactively flag email sending mistakes, such as addressing an email to the wrong recipient.

- Analyzing content for sensitive data relies on the Sensitive Information Types provided by Microsoft, or a custom-definition created by the customer. Sensitive data matching is simple to circumvent to exfiltrate data; the matching algorithms look for exact matches and are easy to trick.

- While a DLP policy can be triggered based on content in the subject line of an email, if the policy action is to encrypt the message then the policy will be without effect because Office 365 Message Encryption passes the subject line through in clear text. It is not encrypted.

- No organizationally-tailored DLP policies are automatically enabled in Office 365; each must be manually configured and fine-tuned. Too few organizations have the cybersecurity skill set available to effectively configure DLP policies. Microsoft has recently introduced new intelligence capabilities that will detect sensitive information that is flowing that should be protected by a DLP policy, and will alert an administrator that some type of remediation action is taken. Whether this soft recommendation approach is enough remains to be seen. There is also a default DLP policy that looks for the presence of one or more credit card numbers sent to someone outside the organization; this is in Policy Tips mode with an alert to the end user.

- DLP policies cannot be targeted to specific groups or regions to help global firms facing different regulatory requirements around the world. The exception to this appears to be for organizations using the new Multi-Geo service, which enables tailoring based on geo (but not necessarily country).

- Documents in SharePoint Online and OneDrive for Business that are identified by a DLP policy as containing sensitive information are blocked in place, to prevent access from anyone beyond the document owner, the person making the most recent change, and the site owner from having access. There is no ability to automatically sanitize the document of sensitive information, or to encrypt the sensitive information within the document while keeping the rest of the document available. Even more significantly, there is no provision that the people beyond the three individuals may have a valid justification for accessing the document with the sensitive information intact. Office 365's block-and-prevent stance may cause problems for valid business processes.

- Actions by an administrator in creating or modifying a DLP policy are not logged to the Office 365 Audit Log. This makes it impossible to know who created a DLP policy and how it has been modified (and by whom) over time.

- DLP policies and sensitive information types cannot identify offending text in scanned images or scanned text. OCR is not supported.

LACK OF SINGLE PANE VISIBILITY ACROSS MALWARE AND NON-MALWARE-BASED ATTACKS

The various threat reports in the Security & Compliance Center provide a piecemeal view of the threats facing an organization across malware and non-malware attack vectors, but not a consolidated view. The various separate reports are focused on specific types of attacks, meaning that a security administrator must manually correlate what is happening across the entire organization in order to gain a "big picture" view.

Office 365 offers the following threat reports via Threat Explorer (Threat Management > Explorer):

- **Malware (in email messages)**
  Shows malware threats that have been detected in email via anti-virus scan, ATP detonation, or reputation detection. Shows top malware families and top users who are being targeted by malware.

The various threat reports in the Security & Compliance Center provide a piecemeal view of the threats facing an organ-ization.

- **Phish**
  Shows email messages containing malicious URLs, and notes how they were detected (by URL, by reputation, by heuristic, or by Machine Learning). Also displays which URLs were clicked, and whether the URLs in question have been blocked or not.

- **User-reported**
  Displays messages that users have reported for re-classification, for example, an email that was delivered but the user believes it is a phishing email or contains malware. Also displays submissions for false positives, in which a user asserts that a message classified as junk is not so.

- **All email**
  Displays a list of all email activity between users and all email messages sent from external sources into the Office 365 tenant.

- **Malware (in files)**
  Lists the files stored in Office 365 that have been detected as malware through the Advanced Threat Protection file detonation process. This includes only files that have been analyzed through ATP file detonation; it is not as assertion about all files in existence (e.g., such as those that have not been detonated or checked).

There is no ability to view a single consolidated list of all threat types, and then to sub-filter using facets.

CREDENTIAL PHISHING AND EMAIL FRAUD

We have identified several issues in Office 365 in the context of credential phishing and email fraud:

We have identified several issues in Office 365 in the context of credential phishing and email fraud.

- Microsoft does not seem to be able to reliably identify credential phishing attempts that lead to an impersonated Office 365 login screen. During 2018, many such emails have been delivered to end users. Since neither the payload nor link itself is malicious, ATP offers no benefit. Microsoft is not consistently identifying impersonated message content for its own service.

- Office 365 will notify the recipient of a suspicious message that spoofs the organization's domain name, but the match must be exact; this is the Exact Domain Spear Phishing Protection service in Exchange Online Protection. Office 365 does not deal with near matches due to similar domains that look or sound similar to the organization's domain (e.g., rnicrosoft.com vs. microsoft.com), and without additional Microsoft cloud services, will struggle to identify email fraud messages that have been sent by compromised internal accounts. With impersonation attacks through the takeover of legitimate mailboxes on the rise, Office 365's lack of advanced detection capabilities is worrisome.

- Protecting users from being impersonated by others requires manual action by an administrator to create an anti-phishing policy and list each specific sender to protect. This list must be kept up-to-date manually by the administrator, since integration with Azure AD based on job roles is not supported – for example, to protect a new Vice President or CEO.

- Traditional methods of classifying spam based on message volume do not work for classifying credential phishing and email fraud messages. The fraud may be perpetuated through only a single message.

- Office 365 does not provide a simple method to remove phishing and impersonation emails from the mailboxes that have passed through filters. Without reverting to PowerShell, there is no way to remove an email across multiple mailboxes and no simple way to revert any retraction (some third-party solutions allow this to be accomplished quite easily). The same problem applies

to DLP in Office 365, since if information is leaked internally there is a need to take action to remove this information. For example, since the *New-ComplianceSearchAction* PowerShell command for purging phishing emails can only soft delete messages, which leaves phishing emails accessible to end users if they recover deleted items via Outlook or Outlook Web Access. Zero Hour Auto Purge (ZAP) only works with spam and malware-based messages, not phishing and impersonation ones.

- Spoof Intelligence manages users, addresses and domains that are permitted to spoof the organization's domain. This provides protection to their own internal users and any business partner or customer who receives valid or invalid email from their domain. Spoof Intelligence is part of the Security & Compliance Center. It should be noted that granular policy control is not available for Spoof Intelligence, instead the feature can only be set to "on" or "off". Additionally, reporting functionality for this tool is limited. Spoof Intelligence was initially released for customers on the Enterprise E5 plan (or those with the ATP add-on), but was made generally available as part of EOP in August 2018.

- Common email authentication mechanisms, such as SPF, DKIM and DMARC, are able to identify brand-spoofing when implemented correctly. They are not, however, so effective at identifying brand-spoofing where look-alike or sound-alike domain names with their own strong email authentication are used. Capturing and appropriately classifying such messages requires going beyond the common email authentication approaches.

SUPPORT FOR HYBRID ARCHITECTURES

The security capabilities in Office 365 offer incomplete support for organizations with hybrid architectures:

- ATP lacks hybrid capabilities, meaning that customers with Exchange or SharePoint on-premises, for example, must have a second and separate threat-protection offering. ATP handles only certain Office 365 workloads under specific conditions, and does not address data and systems beyond Office 365. This can cause problems with many customers operating a hybrid environment.

- DLP policies defined in the Security & Compliance Center apply to specific Office 365 workloads only. These policies are not also enforced for on-premises servers from Microsoft or other vendors.

- eDiscovery in the Security & Compliance Center is only for certain Office 365 workloads, and does not work with on-premises Exchange, SharePoint and OneDrive for Business environments.

The security capabilities in Office 365 offer incomplete support for organizations with hybrid architectures.

Any organization investing in Office 365 security capabilities – with all of their associated issues – will still need to acquire and manage a completely separate set of security services for non-Office workloads and data.

PARALLEL THIRD-PARTY SECURITY SOLUTIONS

Even the best offerings in Office 365 don't address, resolve or mitigate all of the security threats experienced by organizations using the more expensive Office 365 plans (e.g., E3 and E5). For example, phishing emails still get through to end user inboxes, raising risks of credential theft and account compromise. Microsoft prefers to deliver its own monoculture of security services, rather than providing high-functionality integration points for third-party offerings that would bolster overall customer support. At Ignite 2017, for example, Microsoft boasted about its market share of the anti-malware market, claiming to have three times the number of customers than its closest competitor. In the rapidly evolving threat landscape in which organizations find themselves working, both Microsoft and its customers would be better served if Microsoft offered better possibilities for third-party security vendors to deliver complementary security services that bolster Office 365's security

capabilities.

RETRACTION CAPABILITIES

The Outlook client offers a Message Recall capability which can delete or replace a message in a recipient's mailbox under certain conditions. Message Recall is an end-user "best efforts" option in the Outlook client, and is not available in Outlook Web Access nor as an Office 365 service level option. The recall works if the original message has not been read, it remains in the recipient's inbox, the recipient's Outlook client is open, and the recipient is in the same Office 365 tenant. Message Recall has the following limitations:

- It fails if the message has already been read. Both the original message and the recall message will remain in the recipient's inbox.
- It fails if the recipient is in another Office 365 tenant, is not using Outlook, or has moved the message (by automated rule or manual action) into a folder other than the Inbox.
- Recalled messages can be recovered by the recipient, through the recovery of deleted items. Since the recalled message is hard deleted – which moves it into the Recoverable Items folder and not Deleted Items – the recipient can recover those items within the recoverable timeframe.

Documents attached to the recalled message will be subject to the same conditions and limitations. Recall may work, but there are many common conditions under which they will not.

Archiving and Content Management

When considering Office 365, one of the critical questions facing organizations is whether it is a complete replacement for all on-premises Microsoft servers and capabilities, or an addition to current on-premises capabilities.

Within the confines of Office 365, the design intent means the addition of new content sources (e.g., Microsoft Teams) and new content types (e.g., Microsoft Teams conversations, Office 365 Message Encryption, Planner, Stream, and more). This additional content needs to be secured, controlled, and governed.

From the wider perspective, there is also the question of whether the native capabilities in Office 365 provide adequate support for non-Microsoft content sources, and even for Microsoft content sources beyond Office 365.

THERE IS NO EQUIVALENT TO AN EMAIL JOURNAL

Instead of having a conventional email journal, Microsoft has enhanced its Office 365 model to achieve the same "compliance outcome" of a journal service. In short, by putting all relevant mailboxes on Litigation or In-Place Hold, all emails sent and received are retained indefinitely and cannot be deleted by users. Inactive mailboxes (i.e., those belonging to ex-employees) can also be put on Indefinite Hold (currently without a license penalty, however this may change.

If an organization has an existing journal when it migrates to Office 365, it will therefore need a game-plan for either:

- Migrating the existing journal content into Office 365, or
- Moving the existing journal into a third-party journal service and continuing to write to this journal from Office 365

When considering Office 365, one of the critical questions facing organizations is whether it is a complete replacement for all on-premises Microsoft servers and capabilities, or an addition to current on-premises capabilities.

The first option can be achieved with specialist migration software, however Microsoft's guidance on where to migrate journal content remains unclear. There are various limitations on how mailboxes in Office 365 can be used to retain email belonging to multiple users[iv]. Although it is suggested that correctly licensed, shared mailboxes may be used, an organization may have to use many hundreds (perhaps even thousands) of shared mailboxes to accommodate the journal backlog. This makes eDiscovery somewhat complicated and risks exclusion of legacy journals.

The second option means that there is a requirement for two locations to maintain and search in order to meet information governance and eDiscovery needs, but it can result in a lower cost, more practical solution, especially if an organization has years of journals to retain.

ENCRYPTION

Microsoft's first version of Office 365 Message Encryption suffered from numerous weaknesses, including lack of capability, poor reporting, and an inadequate user interface for recipients. At its Ignite conference in 2017, Microsoft announced the release of a new version that addressed some of the weaknesses of the first (including user account and client requirements). However, more than a year after the release of Office 365 Message Encryption Version 2 (or OMEv2 for short), the offering continues to struggle with performance and capability issues. For example:

- The Do Not Forward encryption setting originally released with OMEv2 imposed both encryption and rights management settings on the message and any attachments. Customers found this setting too restrictive for general usage. It is unclear why Microsoft thought that combining the two was a good idea.

- The Encrypt Only encryption setting, released in 1Q2018, in principle addressed several of the criticisms levelled against Do Not Forward, such as the removal of rights management post-delivery. In practice, Microsoft has still not delivered an encryption option that works in Outlook for Windows and Mac with any reliability. Microsoft has had to introduce new tenant-level settings to address post-delivery problems where recipients were unable to read encrypted attachments. The new setting removes the encryption applied to attachments for certain recipients under particular conditions, which appears to undermine the key point of encryption.

- Some Office 365 customers have complained about specific and ever-changing version requirements for Outlook (and bugs in the various versions that mean the service has not worked), the inability to send encrypted messages to other Office 365 tenants under various conditions, and the non-disclosure by Microsoft of tenant-level settings in Office 365 that prevent encryption from working at all.

- Microsoft has attempted to deliver a seamless end-to-end encryption service that works in-line in the Outlook client. It has been unable to do so since the announcement of OMEv2 in late 2017, and there are some indications – such as tying newer capabilities in OMEv2 with link-based messages that open in a viewing portal rather than in-line in Outlook – that it is pulling back on this design goal.

- Encrypted messages sent to recipients using Google Gmail and Yahoo Mail can use their Google or Yahoo identity to decrypt the message in the viewing portal. This is a transparent process for the recipient, but means that if the sender sends the encrypted email to the wrong recipient, the wrong recipient will be able to access the encrypted message using just their Google or Yahoo credentials. The sender and sender organization cannot demand additional identity verification to assure the message has been received by the correct recipient, such as multi-factor authentication. This results in a data breach situation that will be difficult for the sending organization to identify.

Microsoft has attempted to deliver a seamless end-to-end encryption service that works in-line in the Outlook client.

- Likewise, if a user's Google or Yahoo account is compromised, the hacker will be able to use the transparent decryption process to access encrypted messages. This also results in a data breach situation that will be difficult for the sending organization to identify.

- If a recipient's Google or Yahoo account is compromised, the hacker will be able to send encrypted replies to the original sender and other recipients. This could be used for distributing encrypted phishing messages that are more difficult to detect.

- Microsoft's reliance on link-based messages for recipients without Outlook means that encrypted messages can look like phishing messages, especially since they then request a username and password to login. This design triggers all the red flags for phishing attempts. Other email services, such as Gmail, can classify OMEv2 messages as phishing, warning the recipient not to click the link. In other words, OMEv2 messages bear all the characteristics of a phishing message, undermining the ability of the sender to get essential information into the hands of the recipient.

- OMEv2 does not encrypt the subject line of the message. This is always passed through in plain text. This was not offered in OMEv1 either, but if the subject line contains sensitive information, it will not be protected by encryption even if the message and any attachments are encrypted.

- There is no option for an end user to automatically encrypt all messages they send through Outlook. This must be done on a message-by-message basis by an end user.

- As with the original version, OMEv2 offers no post-delivery insights or reporting capabilities for the sender of the message. The Office 365 Security & Compliance Center offers a new report on encrypted messages for Office 365 administrators, but this is not available to end users, and does not report on post-delivery actions by the recipient. This has several implications to workflow, such as the inability of the sender to see if the message has been opened by the recipient. Separate messages or calls are required to confirm receipt. It means that the sender cannot change the encryption status or rights after the message has been sent, and if a sender realizes they have sent a message to the wrong recipient, they cannot know if a data breach situation has occurred or not. Finally, if an encrypted message is marked as spam or filtered as junk mail, the sender has no way of knowing in-band that his or her message was not delivered as expected. Separate messages or calls will be required.

- OMEv2 does not offer the ability for the sender to revoke access to the message after it has been sent from Outlook or Outlook on the Web.

- Microsoft introduced a revocation process in the fourth quarter of 2018 – in preview only – that enables an IT administrator to revoke messages on the behalf of a sender. This requires the administrator to locate the message ID for the offending message (such as through a Message Trace in Exchange Online), and the use of PowerShell cmdlets to complete the revocation process.

- Revocation by an IT administrator is an all-in process – the message is revoked for all recipients. It is not possible to remove access for a specific recipient only, nor to add a new recipient to the previously sent message. This lack of nuance complicates any existing encrypted email discussions flowing from the original, causing a break in workflow for all recipients.

- Generally speaking, OMEv2 offers encryption for Microsoft Office file types only, not for other file types such as PDF. It is focused on organizations using Word, Excel, PowerPoint, InfoPath, and XPS documents. Organizations with non-Microsoft file types in common use will not find OMEv2 of much value. In

There is no option for an end user to automatically encrypt all messages they send through Outlook.

September 2018, Microsoft announced that PDF documents will be supported by the end of 2018. However, the fine print is that while PDF documents will be encrypted in transit, they will not be encrypted once the message is received. This means that PDF documents are handled differently than Office documents, an inconsistency that is sure to lead to data breaches by end users who assume enduring encryption for any email attachment.

ARCHIVING

Archiving – moving business data out of one business system into a separate, secured location for optimized storage, immutability, and better data governance – is not offered for some important content types in Office 365. These include SharePoint, Skype for Business, additional message types, and third-party content.

- 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 become irrelevant. These retention or move actions can be triggered based on specific date-based and event triggers only, and for organizations staying within their assigned storage limits for SharePoint, In-Place Records Management in SharePoint may be sufficient. 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 attracts premium pricing. Organizations with large quantities of SharePoint data are not well served if they want to keep their SharePoint content trimmed and current without incurring additional long-term SharePoint storage fees, or that want to archive content away from SharePoint Online based on event triggers beyond date-based metadata. Moreover, SharePoint is not write once, read many (WORM) compliant – a serious issue for organizations in regulated industries.

- Skype for Business Online relies on Exchange Online for archiving if specific conditions are met. No native archiving service for Skype for Business Online is available. By default, Skype instant messaging transcripts are retained in the Conversation History folder in each user's Exchange Online mailbox, but unless the mailbox is on legal or litigation hold, a user can delete their instant messaging transcripts at will, which doesn't provide an immutable or reliable archive of past messages. The need for legal hold to force the retention of Skype messages means that all Exchange Online mailboxes must be on hold at all times for this to work, which we consider to be an odd design. 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 on BlackBerry devices will be archived into Office 365 if a third-party agreement is in place to capture these messages. Text messages on other devices, including iOS and Android, are not captured. With BlackBerry now having a low market share in comparison to iOS and Android, capturing only BlackBerry messages is not as useful as it might otherwise be.

- Content from specific third-party messaging, collaboration, social media and other content sources can be archived into Exchange Online in Office 365 as converted email messages if agreements are in place with a third-party data partner. Messages are stored in the Exchange Online mailbox belonging to the specific user, and for content that cannot be tracked to a named individual, a catch-all mailbox is used. Most of the context of content from Twitter, Facebook, Yahoo! Messenger, DropBox and Salesforce Chatter is lost when these rich media sources are converted to email messages, making it difficult to re-create a historically valid chain of events.

Archiving is not offered for some important content types in Office 365.

eDISCOVERY

eDiscovery is an essential element for any email and collaboration because of the need to produce information in support of litigation efforts, and because a very large proportion of corporate data is typically stored in organizations' email and collaboration platforms. Office 365 offers some useful capabilities in the context of eDiscovery, but it does have some limitations. For example:

- 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. In practice, searches take much longer to return results.

- 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.

- The advanced eDiscovery capability in Office 365 is not "in-place". The advanced tools provide eDiscovery capabilities within the suite of Office 365 applications and are not integrated directly into the data sources. Therefore, the effort is a two-step process, requiring a search and export for data using the limited Security & Compliance Center capabilities, selecting the advanced eDiscovery center as a destination before one can actually run the advanced tools. Therefore, there is no way to iterate and search on the source data without multiple, manual and repetitive blind operations.

- There are no longer any limits to the number of mailboxes that can be searched. This was the case with eDiscovery in Exchange Online, but has been resolved / removed in eDiscovery in the new Security & Compliance Center.

- Legal holds can be enforced on data in Office 365 locations (many, not all), or on third-party data that has been imported into Office 365 (and is then stored in the user's Exchange mailbox).

Microsoft offers a range of eDiscovery capabilities for searching for responsive material across Office 365, plus a more advanced eDiscovery service called Advanced eDiscovery that adds text analytics, machine learning, and relevance and predictive coding for early case assessment. Advanced eDiscovery is available in the premium Enterprise E5 plan, and as an additional cost add-on to the Enterprise E3 plan. Moreover:

Microsoft offers a range of eDiscovery capabilities for searching for responsive material across Office 365.

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

- An eDiscovery case administrator has no ability within the Security & Compliance Center to send legal hold notification alerts, nor reminders or escalations. These have to be handled out-of-band. As above, the lack of workflow and project tracking capabilities is not ideal.

- Searches for keywords that are started in the Content Search tool cannot be imported into an eDiscovery case. The two services are different and offer no integration. The only way for a search to work in an eDiscovery case is for it to be created within the case.

- eDiscovery cases are made up of holds and searches. No two searches within any eDiscovery case in the organization can have exactly the same name. Office 365 will only permit a given name to be used once in eDiscovery cases across the entire tenant.

- 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, possibly exposing an organization to sanction for insufficient production of evidence.

- It is not possible to configure a more limited search scope for eDiscovery managers searching OneDrive and SharePoint Online repositories, and Exchange mailboxes. Any eDiscovery manager can search any OneDrive folder, SharePoint Online site, or Exchange mailbox anywhere in the world. These should be able to be restricted by geographical region or country to safeguard and protect data.

- It is not possible to set the search scope on email messages to exclude the signature block, so if a keyword appears in email signatures, it will generate a high rate of false positives.

- The eDiscovery capabilities in the Security & Compliance Center take a unified approach to responsive content in three storage containers in Office 365 – user and group mailboxes in Exchange Online, sites in SharePoint and OneDrive, and Exchange public folders. Workloads that store content in these containers can be searched; but other workloads that do not are excluded (such as Yammer, Microsoft Stream, and Microsoft Planner). Further, an eDiscovery case created in the Security & 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 limited approach means that any organization with content outside of Office 365 – including SharePoint 2013 and 2016 on-premises – will need multiple eDiscovery tools, in addition to having to instantiate, perform, and coordinate multiple eDiscovery cases in each separate tool.

- Searching Exchange Public folders is an all or nothing proposition. There is no ability to scope the search to a targeted list.

- 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 are introduced from Office 365 to Azure and then Azure to a local computer – creates unhelpful delays in an urgent process for compliance officers. With GDPR coming on stream in late May 2018, the potential existence of personal data in additional locations will raise significant data governance concerns.

- Exports from Office 365 are not protected and so are at risk of alteration and spoliation. The output is a raw native export and not in a preservation format, such as forensic image format, which many eDiscovery collection tools offer. Moreover, there are no additional encryption options provided by Microsoft to encrypt the export.

It is not possible to configure a more limited search scope for eDiscovery managers searching OneDrive and SharePoint Online repositories.

OFFICE 365 DOES NOT INDEX ALL KEY FILE TYPES

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 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.

Keyword searches may also miss relevant content due to the use of a "best-effort" index. If an organization makes regular use of non-supported file types, it should look at third-party tools that will index additional file types.

SENSITIVE DATA

Office 365 has several limitations when looking for sensitive data in email messages:

- Analyzing content for sensitive data relies on the Sensitive Information Types provided by Microsoft, or a custom-definition created by the customer. Sensitive data matching is simple to circumvent to exfiltrate data; the matching algorithms look for exact matches and are easy to trick. For example:
    - Matching a credit card number can be circumvented by changing any one of the 16 digits into the equivalent word. For example, writing the last four digits as "997four" will not match against the credit card regex (regular expressions).
    - Matching a SWIFT code can likewise be circumvented by changing a digit to a word, or a letter to the Air Force alphabet equivalent. For example, instead of writing the SWIFT code of WPACNZ2W (which will be matched against the sensitive information type), writing it as WPACNovemberZ2W will not trigger a match, and therefore not be caught by the DLP rule. This is even when the email subject line and the email body specify that a SWIFT code is included in the message.
- Even without attempting to deliberately obfuscate the presence of Sensitive Information, messages containing sensitive information are missed by DLP policies if explanatory metadata is missing from the email. For example, an email that contains a Social Security Number but not the explanatory phrase "Social Security Number" does not trigger a DLP policy looking for Social Security Numbers.

Office 365 has several limitations when looking for sensitive data in email messages.

In summary, matching sensitive data requires too much perfection in how sensitive data is formed in a message, and does not use a balanced evaluation for the presence of sensitive data.

NO LONG-TERM STORAGE OF AUDIT LOGS FOR COMPLIANCE

The Office 365 Audit Log only retains audit events for 90 days – for Office 365 subscribers with Enterprise E3 or below. There is no way to increase this time frame. This means the Audit Log can do nothing for an organization trying to track down an issue or problem that occurred outside of the last three months. The exception is audit log entries for Exchange Online, where an administrator can change the default from 90 days for Exchange audit log entries only. For customers with Office 365 E5 and Microsoft 365, audit log entries can be retained for a maximum of one year. This change was introduced to public preview in October 2018, but applies only to audit log records generated after the longer duration comes into effect. Existing log entries are unaffected by the longer retention duration.

The audit logging capability in Office 365 is subject to several issues, including:

- Mail flow events in Exchange Online do not create audit log entries. That is, when a mail flow rule triggers against an email message, no record of this triggering is logged.

- Entries in the Audit Log cannot be put on a legal or litigation hold, in order to show specific actions taken by users over time that are subject to a discovery request or part of early case assessment.

- Exporting audit log items from Office 365 is limited to 5,000 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 information worker. Some medium-sized organizations, let alone their larger counterparts, will hit the 50,000 item limit every day. In such a scenario, an administrator will need to specify and generate at least one export every day, and hope that the time delay in capturing audit report entries doesn't mean that items that should be collected are missed from the report.

- Events are not logged in real-time nor available for real-time analysis. Microsoft says it can take from 30 minutes to 24 hours depending on the specific event that is being logged; customers have noted that it can take even longer and that audit events may never appear at all.

- Exports are delivered as CSV files to be saved locally (outside of Office 365), 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 his or her own wrongdoing; the exported file does not guarantee authenticity of the historical information contained inside.

- The reason for specific actions taken by an admin user on an Office 365 service is not captured and displayed in the Audit Log. It is impossible to piece together the reasoning behind a change based on the general information presented in the Audit Log.

- The Office 365 Audit Log service does not capture events from on-premises Microsoft servers for organizations with a hybrid setup, such as Exchange Server and SharePoint Server in addition to Office 365. It cannot, therefore, provide a consolidated view of auditable activities for organizations with hybrid infrastructure.

In Azure AD, the free and basic editions retain activity and security audit items only for a maximum of seven days. Gaining insight into account compromise, for example, is impossible unless it is identified almost immediately. With a subscription to Azure AD Premium P2, this can be increased to a maximum of 30 days for activity items and 90 days for security items.

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.

In Azure AD, the free and basic editions retain activity and security audit items only for a maximum of seven days.

LICENSING FOR MAILBOXES OF EX-EMPLOYEES

Microsoft has signaled its intent to introduce a new license requirement for inactive mailboxes, originally scheduled to come into force from October 1, 2017. This was going to be priced at US$3 per mailbox per month, or US$36 per mailbox per year.

After receiving push-back from customers and MVPs, Microsoft revoked the introduction of this cost until further notice. It is likely that inactive mailboxes will attract new licensing terms during 2019 or 2020.

Other Issues to Consider

MANAGING HYBRID ENVIRONMENTS

The use of hybrid environments in Office 365 – either on-premises Exchange, other on-premises systems or other cloud solutions – introduces a new set of challenges. For example, Office 365 hybrid deployments introduce a number of disconnected interfaces on-premises and in the cloud that make day-to-day management and automation more difficult. Moreover, the synchronization of identities from on-premises to cloud-enabled rules make it difficult to make changes without complex scripts and highly-privileged accounts. Consequently, tasks that the help desk could do before they can no longer accomplish in hybrid environments, with the result that the increased hybrid administrative burden negates much of the perceived benefit that Office 365 provides.

Organizations that operate hybrid environments – which, according to our research, is more than one in five Office 365-enabled organizations – should use third-party solutions to meet the challenges that will be posed by hybrid environments.

AUTHENTICATION WITH AZURE AD PROVIDES A SINGLE POINT OF FAILURE

As a non-regional service, disruptions in one region to Azure AD can have flow-on or cascading effects to other data centers and regions. While the intent is that Azure AD is globally resilient, Microsoft's architecture for Azure has not yet delivered a fail-safe cloud-based authentication service. For example, a lightning strike in Texas on September 4, 2018 disrupted the cooling systems at the US South Central data center in San Antonio. This had a major impact on both Office 365 and Azure services, with customers outside of the US South Central region experiencing Azure AD authentication problems.

Microsoft's introduction of new capabilities for MFA often breaks current authentication rights, such as preventing affected users from using various Office 365 services. Customers find this annoying and disruptive.

Microsoft's implementation of MFA in Azure and Office 365 delivers a single point of failure. If MFA is down, affected users can't log in, as happened twice during November 2018. Some customers using third-party MFA services with Office 365 claimed to be unaffected by the outages, such as those using Duo and Okta.

SUPERVISORY REVIEW (FOR FINRA COMPLIANCE)

Certain industry regulations, such as those enforced by the Financial Industry Regulatory Authority (FINRA), require the capture and review of communications between particular people, or people in a specific group, to ensure no nefarious or unauthorized topics are being disclosed or discussed. Office 365 previously offered a Supervisory Review capability that could work with Exchange Online messages, which had a range of issues.

In May 2017, Microsoft replaced the legacy Supervisory Review capability with a new Supervision tool that requires the Enterprise E5 plan or the Advanced Compliance add-on. Administrators with the correct access permissions can set up one or more supervision policies.

- Every person who is to be covered by a Supervision policy requires an Enterprise E5 license, or the Advanced Compliance add-on. This is a per-user licensing requirement, not an organizational-level option.
- Supervision works only with Exchange Online in Office 365, but does not address Microsoft's other communication tools, such as Microsoft Teams, Yammer and Skype for Business. This scope of coverage is too narrow in our opinion.

Organizations that operate hybrid environments should use third-party solutions to meet the challenges that will be posed by hybrid environments.

- Once a supervision policy has been set up, a private shared mailbox is provisioned for receiving captured messages. Supervisory reviewers must connect to the shared mailbox to review and assess each message.
- There is no built-in workflow to alert reviewers of a new supervision policy that gives them the ability to review messages. Advising reviewers must be handled out-of-band by the person who set up the supervision policy.
- A person can be set as both the person to put under supervisory review and the reviewer of a given policy. There is no checking to enforce segregation of these roles.
- It is not possible to use Microsoft's sensitive information types in Supervision policies.
- When adding conditions to the supervision policy, the words or phrases must match exactly. A mis-spelt variant will not trigger the supervisory rule. It would be useful if Office 365 offered the ability to use fuzzy matching to give a broader impression of what else what happening through Exchange Online.
- The use of Outlook as the supervision interface means that standard Outlook capabilities - such as creating a new email, replying to a message, and deleting a message - are visible in the interface. Note that the delete option for an individual message is greyed out on the tool bar, and clicking the delete button on a single message surfaces a prompt to say you can't delete the message. Clicking the delete all option on the tool bar deletes all messages in the mailbox, but a background process then puts all messages back into the mailbox. These interface elements are confusing and unnecessary.
- The filter options provided within Outlook don't make sense for supervision. There is no ability to sort and filter messages based on content or metadata relevant to the supervision policy.
- Attempting to delete all messages in a supervision mailbox is not audit logged against the messages.
- A supervisor can reply to or forward a message from within the supervision mailbox. There is no ability, however, to audit or review what messages have been sent from the supervision mailbox.
- Microsoft offers no workflow or case management capabilities for messages in the supervision mailbox. An out-of-band process must be used.
- A reviewer with access to multiple Supervision mailboxes must go through each supervision mailbox one-at-a-time. There is no ability to gain a unified view across multiple supervision policies.
- Aside from the name of the supervision mailbox, there is no indication of what the supervision policy settings are or why messages are being collected into the mailbox.
- Supervisory review works only in Outlook on the web. Although an Outlook client add-in has been promised (and one is available that can be installed, albeit with PowerShell commands), it is non-functional and doesn't work.
- There is no migration support between the old Supervisory Review feature and the new Supervision feature. Policies from the previous approach have to be deleted; they cannot be migrated and updated, and they are not automatically updated by Microsoft.

There is no built-in workflow to alert reviewers of a new supervision policy that gives them the ability to review messages.

- While messages are captured for post-delivery or after-the-fact review, there is no ability to quarantine an offending message and have it routed for approval before release. The damage could already be done, since the message has actually been sent and delivered.

- The Office 365 audit log is blind to supervision policies. Creating, editing, and deleting supervision policies are not audit logged.

Microsoft has made no changes to Supervision since May 2017. Customers with real needs for a robust supervisory review capability should consider third-party offerings.

OTHER ISSUES TO CONSIDER

- Azure AD authentication logs are only retained for seven days for many Office 365 customers. This means that the records of a successful phishing attempt that result in account credential compromise can be impossible to track down, because Azure AD has erased the historical records.

- Office 365 does not support the use of passphrases, which are generally longer phrases containing multiple natural language words that are easier to remember than a password with a difficult pattern. For example, a passphrase could be "I am Clarke Kent and I am Superman." This is a 34-character "password" that is simultaneously easy-to-remember for the end user but, due to its length, harder for an attacker to guess or crack. Office 365 does not support passphrases because Azure AD accounts do not support the use of spaces, and are limited to a maximum of 16 characters.

- New reports on access and authentication cannot be created by admins.

Summary

Office 365 is a robust and capable platform – Osterman Research recommends that organizations seriously consider using it. However, a platform of the scope and scale of Office 365 will never manage to be everything to every organization in every scenario, but the benefits of migrating to the platform must outweigh whatever limitations it includes. As a result, third-party solutions should be seriously considered for deployment, either as replacements for the native capabilities available from Microsoft, or as supplements that will provide enhanced functionality to meet specific organizational requirements.

Sponsor of This White Paper

REFERENCES

[i] https://www.microsoft.com/en-us/microsoft-365/blog/2018/09/24/office-2019-is-now-available-for-windows-and-mac/

[ii] https://www.microsoft.com/microsoft-365/partners/workplaceanalytics

[iii] https://www.fireeye.com/content/dam/fireeye-www/offers/pdfs/pf/email/ig-it-only-takes-one-email.pdf

[iv] https://technet.microsoft.com/en-GB/library/exchange-online-limits.aspx