Osterman Research
WHITE PAPER

**White Paper** by Osterman Research
Published **September 2019**
Sponsored by **Quest Software**

# Using Third-Party Solutions With Office 365

# Executive Summary

Office 365 is licensed for use by more than 180 million users at more than 1.4 million commercial, education and government organizations, making it currently the most popular enterprise cloud service in the world. It covers a variety of situations, scenarios, and capability sets. Microsoft has won massive market momentum by bundling office productivity software and cloud-based services in Office 365 and Microsoft 365, much like it did with its original bundling of Word, PowerPoint and Excel back in the 1990s to create Microsoft Office. This paper discusses aspects of the email messaging and collaboration services that are nearly synonymous with Office 365.

While Microsoft offers an industry-leading communications, collaboration and productivity platform, organizations need to understand their real requirements and most would be well-served by reinforcing the service in several key, supplemental areas, most especially security, archiving, eDiscovery, and encryption. Decision makers need to be aware that relying exclusively on the native capabilities in Office 365 can present challenges and business risks for their organization. While the inclusion of similar capabilities in the platform may give some the impression of platform self-sufficiency, organizations should recognize that certain features may not best align with their business needs, now or in the future. In specific areas, it’s important to recognize that a focused third-party vendor with deep industry and solution experience is often able to deliver deeper and better capabilities compared to Microsoft, thereby complementing Office 365 and reducing the business risk of embracing all Office 365 features as sufficient or even ideal.

## KEY TAKEAWAYS

As with any application, decision makers should perform due diligence on how Office 365 will perform for their organization. This includes:

- Understanding the capabilities on offer in Office 365, and how those capabilities match the organization's security requirements, compliance mandates, and legal processes.

- Undertaking a deep dive on Office 365's features and functions, in order to understand what is and isn't available in Office 365, and how what's available in Office 365 compares to capabilities on offer in third-party solutions that may better address your business needs. Insufficient security and compliance capabilities can result in high threat business events, e.g., data breaches, business email compromise, GDPR fines, ransomware infections, phishing attacks leading to credential theft, theft of intellectual property, and other problems.

- Developing a risk matrix of the security threats and compliance mandates facing your organization, and deciding which risks you are willing to address with standard capabilities in Office 365, along with defining the financial provision that will have to be made if an adverse event occurs. For various other risks, being proactive in establishing more effective safeguards by adding third-party solutions to mitigate the risk will be the better path.

- Planning how to address any identified supplemental needs for Office 365 ideally before rolling out the platform. For organizations where these capabilities are essential, important, frequently used, and necessary to everyday workflow, relying on "good enough" tools is not good enough. Lack of capability starts to have a business net-negative impact. And equally, for organizations where these capabilities are infrequently used, actually having best-of-breed solution sets available is much more important than only "good enough" functionality sets.

***Decision makers must perform due diligence on how Office 365 will perform for their organization.***

## ABOUT THIS WHITE PAPER

Osterman Research conducted an in-depth survey of organizations that are or will be using Office 365, and combined insights from this survey with its own analysis and evaluation of Office 365. Osterman Research provides regular analysis of Office 365 through its Office 365 Analysis Service, available by subscription. This white paper was sponsored by Quest Software; information about the company is provided at the end of this paper.

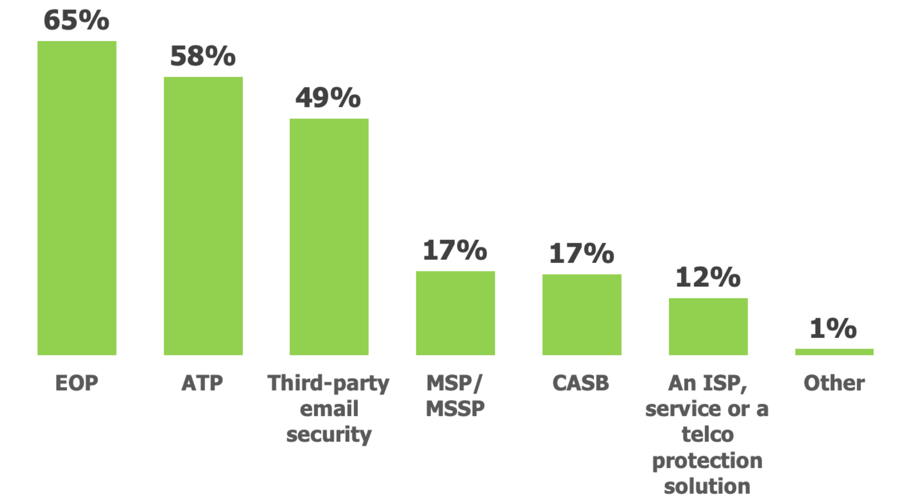
# Issues to Consider for Improving Office 365 Security

Microsoft offers default security capabilities for all customers in Office 365, along with capabilities bearing the "advanced" moniker for the more pernicious threats. Regardless, security threats are still getting through these defenses, in part because native security in Office 365 is not as robust as some third-party solutions (in December 2018, SE Labs found that Microsoft Exchange Online Protection [EOP] achieved only an eight percent effectiveness rating and Microsoft Advanced Threat Protection [ATP] achieved only a 35 percent rating, significantly lower than third-party solutions that were in the high nineties[1].

The use of third-party solutions can result in higher catch rates for spam, phishing, malware and other threats. Third-party solutions with true advanced capabilities also reduce the likelihood that more sophisticated threats – such as Business Email Compromise (BEC) and account compromise – will be successful. The current security solutions used in Office 365 environments are shown in Figure 1.

*The use of third-party solutions can result in higher catch rates for spam, phishing, malware and other threats.*

**Figure 1**
**Current Security Solutions Employed for Office 365**
Percentage of Organizations



*Source: Osterman Research, Inc.*

## ACHIEVING HIGH CATCH RATES

Catch rates for all types of malicious content must be very high because the consequences of malicious content successfully bypassing security layers can be business impactful (e.g., lost staff and management time, lost funds) and even business critical (e.g., business interruption, reputational damage, reduced market value, lost customer confidence, stolen data and intellectual property, regulatory fines under GDPR and similar for not having effective security practices in place). With the increased use of sophisticated social engineering techniques, and the patience of

[1] https://selabs.uk/download/enterprise/essp/2018/dec-2018-essp.pdf

some attackers, it only takes one malicious event to have a significant compromise situation. High catch rates are necessary to protect against:

- Advanced threats that leverage social engineering techniques, post-delivery weaponization of attached payloads and URLs, and business email compromise to perpetuate fraud. The intention here is to stop or make safe such social engineering attacks to prevent the user becoming compromised, avoiding the subsequent loss and recovery cost.

- Ransomware that cripples business operations through malicious encryption, and other types of malware that exfiltrate data for sale, exposure, or to use as part of credential phishing campaigns.

- Fileless malware that executes in memory and doesn't leave any trace on disk. Such approaches have been effective at bypassing anti-malware techniques that only analyze what is happening on-disk.

- Evasive phishing campaigns using new techniques to avoid detection by existing, automated security solutions.

- Graymail, which some users want and others no longer want to receive. Graymail is not usually a carrier of malicious content, but for some users receiving graymail is an annoyance.

## AZURE AD AND OFFICE 365 AUDITING

While Microsoft owns the platform, customers are still responsible for the activity of their users, and so insider threats are still possible. The Azure AD Audit and Sign-in Logs via Azure Portal, and the Unified Audit Log in the O365 Security and Compliance Center, have some limitations for insider threats. These include difficulty in searching and interpreting the logs that are generated, multiple consoles/screens, no single correlated view of on-premises and cloud activity for organizations with hybrid environments, and short retention periods for audit logs that put customers at risk for compliance retention and investigations.

## IMPROVING INBOX SECURITY

Pursue a strategy of email defense-in-depth by adding an additional layer of security with one of the new offerings in the emerging category that Osterman Research classifies as "Inbox Detection & Response" (IDR), and which Gartner recently referred to for the first time as "Cloud Email Security Supplements." These are normally intended as a complement to any existing gateway security, and are being provided by third-party security specialists who are integrating with Office 365's native API to continuously inspect emails that have already been delivered. Some offerings include functionality to automate the removal of emails found to be malicious, with the primary use case being the remediation of phishing emails missed by gateway security, and can incorporate some sort of automated framework for users to rescan or submit suspicious emails.

## ZAP MALICIOUS CONTENT REMOVAL

Once malicious content is identified in a mailbox, it should be possible to remove all instances from all mailboxes. Office 365 offers Zero-Hour Auto Purge (ZAP), which only partly addresses this requirement. ZAP will automatically move a newly classified malicious message from a user's inbox to their Junk folder, but cannot delete it permanently or move the offending message to the quarantine, meaning the user still retains access through their Junk folder. Office 365 also offers PowerShell options for completely deleting malicious content, but if scoped incorrectly, this can completely delete valid content from user mailboxes.

***Office 365's ZAP feature only partially addresses the requirement for removing malicious messages.***

## CO-EXISTENCE OF SECURITY SOLUTIONS

A common refrain in the security industry is the need for cross-vendor collaboration and multi-solution coordination, because no single vendor is ever going to catch and prevent all threats. As confirmed by post-delivery analysis of threat-bearing emails that were checked by Microsoft's tools, but still delivered to the user's inbox, there is a great need for effective co-existence of security solutions. For example, Microsoft's tools frequently miss emails from compromised accounts, and often allow delivery of fake Office 365 announcements and billing demands, which, if successful, lead to account compromise. Third-party solutions from specialist email security vendors include innovations that complement and extend the native EOP and ATP security tools in Office 365.

## ADD A LAYER OF INBOX SECURITY

One option for pursuing a strategy of email defense-in-depth with Office 365 is to add an additional layer of security with one of the new offerings in the emerging category that Osterman Research classifies as "Inbox Detection & Response" (IDR), and which Gartner recently baptized as "Cloud Email Security Supplements." These are normally intended as a complement to any existing gateway security, and are being provided by third-party security specialists who are integrating with Office 365's native API to continuously inspect emails that have already been delivered. Some offerings include functionality to automate the removal of emails found to be malicious (see also Malicious Content Removal below), with the primary use case being the remediation of phishing emails missed by gateway security. Another feature to look for is the incorporation of some sort of automated framework for users to rescan or submit suspicious emails for evaluation.

## CREDENTIAL PHISHING

Credential phishing is an increasingly common attack vector. If an attacker can secure valid credentials, further concealed attacks can be executed and hidden from sight. In evaluating your security needs, look for capabilities to detect near-match spoofing of domain names, because attackers will craft domain options that look similar to a distracted human eye, or even worse, that are hidden completely from display on mobile devices. When internal accounts have been compromised and the message header settings are perfectly valid technically, other non-message header signals must be assessed and correlated in order to identify the attempted fraud. People have higher trust for internal messages from known accounts and known people, and carefully planned internal attacks via compromised accounts are often nearly impossible for a recipient to identify.

***Look for specific delivery SLAs for sandboxed messages.***

## THINGS TO CONSIDER WHEN EVALUATING ADVANCED THREAT CAPABILITIES

Organizations are under attack from targeted and advanced threats and effective defenses are essential. Consequently, it's important to evaluate whether Office 365's native security capabilities versus those of third-party solutions will meet an organization's requirements. Consider the following:

- All necessary file types should be checked for threats, not just Office file types that are the predominant area of interest for Microsoft[2]. Attackers are not limited to the file types created by Office 365 applications, and thus for organizations using more than Office file types in daily business interactions, supplementing what Office 365 offers is essential.

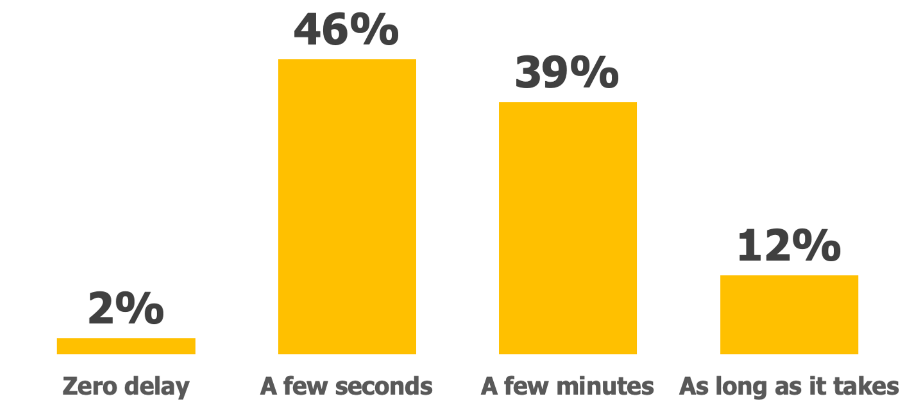
- Dynamic scanning or time-of-click URL checking should work for all links clicked by an end user, rather than being limited to URL links in Outlook email messages and Office documents. When users have access to make types of files, Office 365 ATP Safe Links will be silent. Also, there is a need to ensure clicks can be followed where "multi-hops" are in place, otherwise malicious intent can be hidden from scanning. Where a link is unknown, and potentially risky, isolation of weblinks is an effective technique to allow users access in a way that keeps them safe from potential infection or phishing compromise (read-only website view).

[2] 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).

- Intelligence on newly-identified threats in an email should be shared beyond the original inbox as close to real-time as possible, so that any other instances across the network are neutered before causing havoc. Microsoft offers signal sharing and correlation in its Intelligent Security Graph, but the time delay and effectiveness of this signal sharing is unclear.

- Vendors should specify a maximum guaranteed delivery time for scanned and sandboxed messages, with specific SLA reporting. In an attempt to reduce the delivery time, Office 365 has introduced various configurable options for administrators to turn on or off, but it is always in the context of "best efforts" and never against a tracked benchmark. The performance and stability of ATP is bundled with more general Office 365 Health Status Indicators, hence there is no structured way to assess trending performance status. The tolerable delay in email delivery for increased security processing is shown in Figure 2. Nearly half of organizations consider a delay up to only a few seconds acceptable.

**Figure 2**
**Tolerable Delay for Increased Security Processing**
Percentage of Organizations



*Source: Osterman Research, Inc.*

**Next-generation advanced detection mechanisms should be included in Office 365.**

- Next-generation advanced detection mechanisms should include deep content inspection, recursive analysis of embedded documents, evaluation of threats below the application and operating system levels, and identification of dormant code. Sandboxing on controlled physical machines should also be available to analyze for malware that has been intentionally designed to evade virtual sandboxing detonation mechanisms. Microsoft offers several advanced detection capabilities in Microsoft Defender ATP (originally Windows Defender ATP for Windows-only), but this is part of a Microsoft 365 subscription not an Office 365 one.

- Advanced disarming capabilities such as deep content filtering or CDR (content disarm and reconstruction) should be considered to neutralize threats within attachments and inline files. These solutions effectively handle zero-days and unknown threats compared to legacy detection-based technologies that are easily evaded by sophisticated attackers. All incoming files should be disarmed before the user is given access to them to ensure that files are malware-free.

- Disarming solutions available in the market are fast and cost-effective compared to legacy detection-based technologies and should be considered. The average latency for file handling via legacy detection solutions could reach a few minutes while disarming technology tools enable latency of just a few seconds for file handling.

- Finally, robust defenses against CEO Fraud and BEC attacks are essential elements of a security solution. While Office 365 offers defenses against such attacks, they are less refined than those offered by third-party vendors. For example, the Anti-Phishing Policy in E3 only supports management of anti-spoofing settings, while the ATP version of the Anti-Phishing Policy in E5 adds impersonation protections. Note that domains must be explicitly declared for impersonation protection in the ATP version, but it is unclear how effective the reactive setting is against homograph domain attacks (including look-alike and sound-alike domain names). Some third-party solutions offer proactive protection against homograph domain attacks, among other advanced capabilities. In the same way, Office 365 does not offer email writing style analysis as part of its detection methods for BEC attacks. When a BEC attack circumvents the anti-phishing policy for an Office 365 customer, it is up to the recipient to judge the validity of the message contents. Third-party solutions can strengthen such judgments with AI-enabled analysis of the writing style of a new email against a previously trained model of the supposed sender's writing style. If the two don't match, alerts are triggered. Checks of this nature are not offered in Office 365.

## ENSURING PROPER SECURITY CONFIGURATIONS

Threat protection should be enabled by default, rather than being dependent on an administrator configuring a complex set of policies to address the range of threat scenarios facing the organization. For example, while Microsoft's Advanced Threat Protection (ATP) module for Office 365 offers the possibility of checking attachments and links for unknown and emerging threats, an administrator must set up policies to apply these capabilities to individuals, groups and the organization before any added safety is enabled. No threat protection is on by default, and even when it is on, users must be connected to Office 365 in order for Safe Attachments and Safe Links to work.

***Threat protection should be enabled by default, rather than being dependent on an administrator configuring a complex set of policies.***

## ANTI-SPAM TECHNOLOGIES

The native spam filtering in Office 365 does block considerable spam, but there are certain characteristics and constraints customers should take into account, including:

- The spam quarantine should share intelligence with users on the prevalence of particular spam messages or variants. When users access their quarantine in Office 365, a post-delivery analysis of how other users classified such messages is not shared, leaving each user to make their own decision on the validity or otherwise of individual spam messages.

- Quarantined spam messages should be retained for as long as admins determine is appropriate. While Office 365 increased the maximum timeframe to 30 days in September 2018, admins do not have the option to increase the limit beyond 30 days.

- When users review messages in their spam quarantine, Office 365 does not offer the option of a workflow process where an administrator can verify the safety of a message before releasing it to a user.

- Admins should have the ability to create different policies to deal with different types of spam, bulk messages and graymail. Office 365 provides the ability to create policies that differentiate based on who such messages are sent to, but not on the type of spam nor its severity or rating scale. For example, all spam must be delivered to a singular location for a given recipient set, instead of being able to direct different levels of spam to junk, the quarantine, or deleted items. Office 365 goes part of the way towards this with a differentiation between spam and high confidence spam, but there are no other spam severity settings available. Likewise for bulk email; it's all to one place for a defined recipient set.

- Once a user has made the decision to block a given sender, future messages from that address should be deleted immediately. But that is not the case in

Office 365. Messages from blocked senders are still sent to the spam quarantine. This overloads the quarantine with possible spam as well as email from blocked senders; it would be much better just to have emails that have not been sent from blocked senders shown in the quarantine.

- Notifications about spam and other quarantined content should be customizable by admins, particularly with regard to frequency and time-of-day. Office 365 does not work this way; notifications are sent when Microsoft decides to send them, and since no attempt is made to be time-zone aware, many people receive quarantine notifications out of work hours. The minimum frequency is daily, and it is not possible to send a notification for each message received.

## MULTI-SOLUTION INTEGRATION

Different security tools focus on identifying and neutralizing specific types of threats, and while focused capabilities are beneficial, integration across multiple tools gives security analysts the big picture. Relevant considerations for Office 365 platform users include:

- Monitoring all security solutions in use from a single interface makes security staff more efficient. The Threat Management section of the Office 365 Security & Compliance Center offers monitoring of email- and content-borne security threats, while other Microsoft security solutions are monitored in Office 365 Cloud App Security (in E5 plans) or Microsoft Cloud App Security (in Microsoft 365 plans). The new Microsoft 365 Security Center may address the current division of monitoring capabilities, but this is still a work-in-progress.

- Security solutions should be able to monitor security capabilities across all cloud-based and on-premises solutions. The tools in Office 365 are Office 365 centric, and unless higher priced plans are acquired, offer no insight into on-premises solutions and security threat events in other cloud services. Microsoft has recently introduced a new cloud-based SIEM - called Azure Sentinel - that is expected to deliver an integrated monitoring service, but this is not included in Office 365.

- A single, consolidated list of all threat types should be offered to improve a security analyst's overall understanding of the changing threat landscape. Threat Explorer in Office 365 only offers filtered slices of threat data – for example, malware, phishing, and user-reported – but not a consolidated list.

***The effectiveness of DLP requires more nuance than brute force approaches offer.***

## DATA LOSS PREVENTION

DLP is a defensive technology that analyzes content containers in-motion and at-rest for content that violates policy. For example, an outbound email message that contains sensitive customer data should either be blocked entirely, encrypted to limit access, or sanitized through redaction before release. However, DLP applies not only to email, but also to the sharing of files via OneDrive. Proper DLP in Office 365 environments should include inline and offline capabilities – available from third-party vendors – to properly address potential violations.

Issues to take into account in using Microsoft's DLP capability in the E3 and E5 suites:

- DLP solutions should work across all of the file types and applications that an organization uses, rather than just focusing on the Microsoft Office applications. Without this broad level of support, data is more likely to be lost as people carry out standard business tasks through non-Office file formats. DLP policies that trigger on a Microsoft Word document, for example, will fail to identify an Apple Pages document with the same content inside.

- Vendors should offer an extensive set of standard DLP policies out-of-the-box, so that the organization immediately gains a baseline of protection against data loss. While Microsoft now offers a basic DLP rule to identify credit card numbers in email messages, no other out-of-the-box policies are offered in Office 365. It's important to note that simplistic approaches can trigger false positives (e.g., valid 16-digit numbers like SKU codes could be mistaken for credit card numbers).

- Organizations working across multiple legal jurisdictions and geographical regions require the ability to tailor DLP policies for specific situations, rather than having all-of-business policies. Organizations subscribing to Multi-Geo in Office 365 are able to leverage these capabilities, but otherwise such capabilities are not available.

- Some third-party add-on apps can lead to data loss and compliance risks in the cloud if they have broad permissions to access enterprise data. In some cases, these OAuth-enabled apps can be malicious or they can be used for persistent data access by threat actors after an account has been compromised.

- Stop-and-block DLP systems apply brute force to prevent an email containing sensitive information being shared, but more nuanced approaches enable both policy-based encryption of the complete message as well as automated redaction of sensitive information. Without the more nuanced options available, end users and administrators must invest more time in manual rectification steps, slowing the spread of valid messages and content.

- Document fingerprinting identifies standard business forms that are likely to contain sensitive or confidential information that should not be shared freely. Office 365 supports complete document fingerprinting when all of the fingerprinted cues from the original document template are present, but will not trigger if only a partial match is made. A business form could be cut in half, for example, with each half sent in a different email message to avoid detection by the DLP rule. Some third-party DLP vendors use a different approach for creating the original document fingerprint in order to more reliably identify full and partial matches of the fingerprint.

- Messages that violate DLP policies should be routable to a role, not just a specific individual. Supporting this nuance enables the right supervisor or manager to review the message for sensitive information, in light of their greater awareness of the context surrounding the content that is invariably invisible to a security administrator.

- While DLP policies can prevent sensitive content being shared with the wrong recipients, they lack the nuance to detect when a sender is sending something to the wrong recipient accidentally. While the message may be encrypted by policy, for example, it will still be delivered to the wrong person. Advanced DLP offerings should be able to detect when content is being sent to someone who has never been sent such content before, when someone is sending content that's usually sent internally to an external distribution list, or has selected a distribution list that they don't normally use.

- 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.

- Actions by an administrator in creating or modifying a DLP policy should be centrally logged for subsequent review and analysis. While Office 365 logs matches of DLP policies, the actual creation and editing of DLP policies are invisible to the Audit Log. This means there is no way to see who created or modified a policy, and when.

***There are no workflow options for messages and files that violate a DLP policy.***

- Identifying content hidden in image files should be supported by a DLP solution, so that circumvention isn't just as simple as scanning an offending document to an image file. OCR capabilities in some third-party DLP solutions detect content in images and trigger DLP policy matches, a capability not available in Office 365.

### EMAIL RETRACTION

When emails are sent in error, the ability to retract an email limits data loss and prevents embarrassing mistakes from becoming fodder for public discussion. Within a given Office 365 tenant, there are some options for message retraction if the message is unread, and some PowerShell commands to locate and delete offending messages across mailboxes. The latter must be used with extreme care, because wrongly scoping the PowerShell command will lead to undesirable data loss. Once a message has gone outside of a given Office 365 tenant, however, there is no automated ability to retract the message. All that the red-faced sender can do is send a follow-up email requesting deletion, but the execution of this request is solely at the judgment of the recipient. Often highlighting the message sent in error does more to elevate its interest than achieve the deletion request.

## Issues to Consider for Improving Office 365 Archiving and Content Management

Microsoft has a particular approach to archiving and eDiscovery that suits its Office 365 and Microsoft-centric view of the world. However, the use of third-party solutions can offer a better archiving and eDiscovery experience, in line with the business and compliance requirements of the modern organization. This is especially relevant for archiving and eDiscovery around business records that do not originate in Office 365.

### ARCHIVING

While many organizations are moving in the direction of embracing as much of Office 365 as possible, few are exclusively using Office 365. The majority of organizations have additional information systems, digital tools, and repositories of data. Organizations need to manage this complex information space in line with business, legal, and information management requirements. Important considerations in this respect for Office 365 platform customers include:

*Content should be archived in its native format to preserve all content signals and metadata.*

- An archiving solution should be able to capture and store all business-relevant content types and make these available through an integrated interface. Email is the big ticket item for digital archiving, but not exclusively so. As organizations embrace newer communication and collaboration tools such as instant messaging (e.g., Skype for Business and Microsoft Teams), collaboration systems (e.g., Microsoft Teams), and enterprise social networks (e.g., Yammer), the ability to archive this content becomes increasingly important, although even within Office 365, not all Office 365 content types are archivable. Other content types - external social media posts, text messages, voicemail and any other content that falls under archiving's purview - must equally be captured and stored in an integrated archiving environment. In recent years, Microsoft has offered the ability to integrate some third-party content into Office 365 using third-party integration specialists, and more recently has introduced its own tools for this integration. Check to see if the Office 365 and third-party content types used within your organization are supported for archiving.

- Content should be archived in its native format to preserve all content signals and metadata. Microsoft's approach is contrary to this principle, however, as any third-party data imported into Office 365 is converted into an Exchange email format for storage. For example, a Facebook post is converted into an Exchange email for archiving, an approach that suits Microsoft's legacy technology but not modern requirements.

- Archiving solutions should integrate into a central view for compliance managers, legal staff, and senior management, among others. Office 365 enables content search against current and archived data, but does not offer a view of all archived data. Archived data can be searched, but not browsed.
- Some organizations require the creation of a central location for archived data, while others prefer in-place archival. Office 365 only offers in-place archiving for Office 365 data, along with any third-party data imported into Office 365 and converted into an Exchange email format. Office 365 does not offer archival via content movement, a capability that is available from third-party vendors.

- Separate retention, preservation and disposition policies for a user's mailbox and archives should be available to support more granular or nuanced archiving requirements. Office 365 offers policies that apply universally across a user's mailbox and archives, with no option of policy differentiation. Some third-party vendors offer more granular options.

## eDISCOVERY

Legal investigations require the ability to search for responsive content across relevant content systems in the organization, and the ability to lock content to prevent deletion or modification until the legal investigation has concluded. Effective eDiscovery capabilities are a core requirement at such times. Organizations require the following:

- An eDiscovery tool should be able to search across all corporate data repositories, including those delivered via cloud services (such as Office 365) and via on-premises servers and solutions. The eDiscovery tools in Office 365 do not offer this capability. They can search some of the data originally created in Office 365 (several workloads in Office 365 are not covered by eDiscovery searches), as well as any third-party data that has been imported from third-party systems and converted into an Exchange email format, or for customers with Advanced eDiscovery in Office 365, content that has been uploaded into Azure. Any content in systems outside of Office 365 is non-addressable by an Office 365 eDiscovery search.

- eDiscovery case administrators should be able to send litigation hold notification alerts, reminders and escalations using native capabilities of the platform, rather than having to resort to out-of-band communications. Having the ability to see when and to whom these were sent within the context of an eDiscovery case gives evidence that due process was followed, and provides clarity on current status and next actions for any case administrator. The standard eDiscovery tools in Office 365 do not offers these capabilities, although the new version of Advanced eDiscovery for E5 customers offers Custodian Management for initial and further communications.

- Content and eDiscovery searches should come with an SLA, rather than a best-efforts approach that repeats generic statements about ever-increasing speed. Microsoft claims that average search times are being reduced all the time, but no SLA is offered for eDiscovery searches.

- eDiscovery tools should be able to query data in-place, without requiring a content export from the original content system and subsequent importing into Office 365 or Azure (for Advanced eDiscovery searches). eDiscovery content searches can search most Office 365 content in-place, but not any content beyond Office 365. Any non-Office 365 content must first be imported into Office 365 or Azure for analysis.

- Litigation holds should be enforceable across all content systems, including Office 365, cloud services, and on-premises locations used by the organization.

***An eDiscovery tool should be able to search across all corporate data repositories, including those delivered via cloud services...and via on-premises servers and solutions.***

Preventing deletion and modification of content in source systems preserves actual business records and interactional dynamics, rather than an imported manifestation of the same. eDiscovery tools in Office 365 can place litigation holds on the major workloads in Office 365 (but not all workloads), and do not extend to non-Office 365 locations even if these are based on Microsoft's on-premises server tools.

- The ability to define the format of content to be produced in response to an eDiscovery request should be possible. While native-format files are often preferred by the requesting party - and supported in Office 365 - producing in different formats that reduce fidelity or exclude full metadata can make a difference to the legal outcome of the case. Third-party eDiscovery vendors often support additional production formats, in addition to native-format files.

- Content exports of eDiscovery searches into third-party review tools should be protected from spoliation, for example by using a forensic image format. This is not available in Office 365, with copies of emails and documents being downloaded for import, along with a spreadsheet of exported case data. This export set could be manipulated prior to importing into a review tool.

- Project tracking and workflow capabilities should be available for eDiscovery cases, so that when multiple people are working on a case, it is clear who is doing what by when. Tracking capabilities are not available in the standard eDiscovery tools in Office 365. The new Advanced eDiscovery release of 2019 adds new case management tools, but these only enable a shared list of tasks to complete rather than supporting task assignments.

- Admins should have the ability to create case templates for repeatability and auditing, with standard search queries and locations, key actions and requirements to complete, and an audit trail of what was and was not performed. Office 365 provides the ability to create new cases from scratch, but no ability to create templates to streamline future efforts and codify learning.

- eDiscovery content searches confer great power to locate sensitive information across the information space within an organization. Multi-national, multi-business and multi-region organizations often require the ability to restrict the search scope of given eDiscovery users to enforce compliance boundaries. Microsoft offers some capabilities for setting up compliance boundaries, but this requires the intervention of Microsoft Support and the use of PowerShell to create search permission filters. Nonetheless, eDiscovery users are still able to select any repository across the organization when constructing a content search, although the search results themselves will be limited to the boundary created.

- eDiscovery searches should be able to be configured to ignore certain content parts of available content items. For example, standard signature blocks in emails should be able to be excluded from an eDiscovery search, and other boilerplate text in emails and documents should be able to be ignored as well. eDiscovery content searches in Office 365 do not support these exclusions and search restrictions, which results in false positives when a search term is located in the signature block or boilerplate text.

***Microsoft enhanced the capabilities in Office 365 for creating logical boundaries to separate content locations that eDiscovery Managers can search.***

## COMPLIANCE BOUNDARIES

Government and industry regulations dictate standards of behavior from organizations and mandate that certain rights are honored and various capabilities made available within technology and organizational processes. The ability to comply with key elements of data privacy regulations – with the European General Data Protection Regulation (GDPR) as the prime example - should be easy to support and appropriate to the actual requirements specified.

Microsoft enhanced the capabilities in Office 365 for creating logical boundaries to separate content locations that eDiscovery Managers can search. The same controls can be used to limit who can access eDiscovery cases. The intent is to support organizations who must comply with different regulations in different geographical areas, such as multi-national corporations and governments made up of multiple agencies.

Compliance Boundaries are enabled using PowerShell, via the search permissions filtering cmdlets. There are several relevant issues Office 365 platform customers should be aware of:

- An organization wanting to create compliance boundaries must first nominate a user-level attribute in Azure AD that can be used to divide individuals into separate logical groupings, such as by department, company, office, or other. Microsoft has a specific list of attributes that can be used, in order to enable support across Exchange, SharePoint and OneDrive. Clearly, good processes will need to be in-place to ensure the nominated attribute is kept current for all employees.

- A support request must be filed with Microsoft Support to sync the nominated Azure AD attribute to all OneDrive accounts. This will also map the attribute to SharePoint as a hidden managed property. The completion of this support request can take 4-6 weeks.

- Role groups must be created in the Security & Compliance Center, in order to divide people with eDiscovery Managers rights into separate groups for accessing the separate agencies, departments or other groupings. When a new eDiscovery case is created, the correct role group needs to be given access rights.

- A PowerShell cmdlet is used to tie together a nominated attribute value and a specific eDiscovery Managers role group.

- For organizations using Multi-Geo, an additional parameter in the cmdlets can also be used to specify additional search constraints and which datacenter is used for exporting data. This provides further capability to keep relevant data within a specified geographical boundary. The use of Multi-Geo with compliance boundaries also introduces some implications for the search rights of eDiscovery Managers.

- There are still some anomalies that Microsoft needs to fix over time. For example, while the cmdlets will prevent the return of search results of content locations in a different boundary, an eDiscovery case can still include content locations beyond the boundary. The boundary is enforced below the level of the user experience, which could lead to confusion as a consequence of eDiscovery Managers selecting locations they don't actually have permissions to search. Secondly, compliance boundaries are ignored for legal holds, meaning that an eDiscovery Manager in one boundary can still put users in other boundaries on legal hold. Third, compliance boundaries do not apply to Exchange Public Folders.

***There are still some anomalies that Microsoft needs to fix over time.***

Having a structured way to enforce logical boundaries between content is important for large, complex organizations when moving to the cloud. The architecture of a single worldwide tenant with or without Multi-Geo support comes with the requirement to create boundaries in some way; previously this would be done with separate physical infrastructure and therefore separate physical boundaries in an on-premises world.

Since the user-level attribute offers a real-time status of the boundary affiliation of a user, it is unclear how Microsoft handles eDiscovery searches for previous time periods where the user was affiliated with another boundary. For example, if a 2019 case requires searches against Department1 data locations from calendar year 2017 when User1 was in that department but User1 moved to Department2 in 2018, will User1's data sources still be searched? It would appear the answer is no, and therefore potentially responsive material will be excluded by design.

### SUBJECT ACCESS REQUESTS

Article 15 of GDPR provides right of access by a data subject to two things: firstly, confirmation of whether or not personal data concerning him or her are being processed, and if so, secondly, access to that personal data and various additional information, such as the purposes of the processing, the categories of personal data concerned, and data storage periods, among others. The context and scope is personal data, as defined in Article 4(1), which includes a name, ID number, location data, an online identifier (e.g., user name), or other specific factors about the identity of the person.

The capabilities provided by Microsoft in Office 365 for handling data subject requests, by contrast, produces a collection of email messages and documents (by default) that were created by or addressed to a data subject by searching for their name, instead of insight into personal data about the data subject. Data collected by the data subject request can be re-scoped by changing the search query to reduce the quantity of data included, but must be exported for review (which then creates a separate exported data set that sits outside of the data privacy controls in Office 365). This brute force approach to identifying data created by or addressed to a data subject goes far beyond the requirements of GDPR, and results in an onerous task for manually reviewing all exported messages and documents. Further, Microsoft's approach is likely to include personal data on other data subjects (and thus could trigger a data breach situation by releasing the artifacts to the original requestor), and is also likely to hand-over confidential and secret business information about the organization merely because the name of the data subject was included as the author, contributor or otherwise involved. Office 365's data subject request tool identifies and exports data authored or created by a data subject, rather than identifying personal data about a data subject.

### RIGHT-TO-BE-FORGOTTEN

Article 17 of GDPR gives data subjects the right-to-be-forgotten or right of erasure for personal data. This right can be exercised under certain conditions (e.g., that the reason for the personal data being collected has lapsed, or that the data subject withdraws their consent for the processing of their personal data), but can also be rejected by a data controller under certain conditions (e.g., that the data must be retained to meet a legal obligation or assist with a legal claim). In other words, there is a lot of nuance at play, which poses challenges to organizations using poor practice approaches for storing personal data (e.g., Excel spreadsheets with HR data) and to Microsoft for its ability to provide tools to organizations that identify personal data that only falls within the boundaries of the specific erasure request. There are no automated tools offered in Office 365 to help organizations comply with Article 17 rights; everything will require tedious manual review.

## Issues to Consider for Improving Office 365 Encryption

Encryption solutions protect email messages and documents from unauthorized access. Microsoft offers native encryption capabilities in Office 365 that focus mainly on supporting Outlook emails and Office documents, but some third-party encryption solutions add richness and capability that is missing from Microsoft's offer. Issues that Office 365 customers should consider include:

- Encryption capabilities should be integrated with the places where people work, such as Outlook for Windows, Outlook for Mac, and Outlook on mobile devices.

***Microsoft offers native encryption capabilities in Office 365 that focus mainly on supporting Outlook emails and Office documents.***

Users should have the ability to automatically encrypt all messages or only manually encrypt certain messages. Recent releases of Outlook in Office 365 ProPlus included integrated encryption, and the ability for a user to manually select encryption for a given message. Automatic encryption of all messages as a user-level setting in the Outlook client is not available, and while Outlook mobile supports in-line decryption of encrypted messages, there is no ability to send an encrypted message with a manual action in Outlook mobile.

- All document and file types in use within the organization should work with your encryption solution, and all encrypted attachments should work the same way. Third-party encryption solutions offer broader coverage of file types, compared with Office 365 which focuses on Office documents and Adobe PDF. Note that PDF documents encrypted with Office 365 Message Encryption are handled differently after delivery then Office documents.

- Once an encrypted message has been sent, senders should be able to revoke or change the encryption status of a message after delivery on a per-recipient basis from the Sent folder in Outlook. Office 365 does not offer this capability to senders. Note that the 2019 edition of Advanced Encryption - available in the higher priced Office 365 plans - enables an administrator to revoke a message under two conditions. First, the message must have been sent to an external recipient who doesn't also have a guest user account in the tenant. Secondly, it must be a link-based message, not one that supports in-line decryption in Outlook. Revocation does not work for internal users in the Office 365 tenant, and does not work for non-link-based encrypted messages. The administrator can use PowerShell or the message encryption report in the Security & Compliance Center to revoke a message, although there is a delay of about a day for messages to be listed in the encryption report (which seems tediously long).

- Sending an encrypted message prevents unauthorized access beyond the person to whom the message was sent, but if the wrong recipient was selected by mistake, or the correct recipient's account has been compromised through a phishing attack, a data breach situation can still happen. Senders should be able to request additional identity verification so that only the correct recipient is able to view the message, such as via a multi-factor authentication test. Additional identity verification options are not available in Office 365, and when combined with the lack of reporting available to message senders, means that no information is available to give warning of inappropriate access until it is too late.

- An encryption solution should provide non-link-based message sending options to avoid encrypted messages looking like phishing messages. While Microsoft has pushed in the direction of in-line in-client message display, many of the recent "innovations" have represented a pulling back to link-based messages, especially in the business-to-consumer space. Given the infrequency with which people receive these, they could be used to as a phishing vector - especially if people get used to supplying credentials to view the message.

***An encryption solution should provide non-link-based message sending options to avoid encrypted messages looking like phishing messages.***

- The subject line of an encrypted message should be encrypted, not passed through in clear-text. There is no option to encrypt the subject line in Office 365 Message Encryption, which means that any sensitive information in the subject line itself will remain unprotected.

- Post-delivery reports should be available to senders and admins to determine if encrypted messages were received by the recipient. Since post-delivery actions are required in the message to determine recipient authenticity, some signals must be available on receiving status, but none of these are made available to senders. Reporting is available for administrators on messages that were sent, but no intelligence on whether the message was delivered, marked as spam, or opened by the recipient. An administrator can revoke a message if it is a link-based version accessible through the Office 365 web portal. Revocation is not available for messages delivered to an Outlook client with in-line decryption.

## Other Issues to Consider

We have reviewed important aspects of Office 365 across security, compliance, archiving, eDiscovery, and message encryption above. Four additional issues to consider are discussed in this section:

### STORAGE OF AUDIT LOGS

Audit log entries should be stored for as long as an administrator wants to retain them, including indefinitely. While the higher-priced plans in Office 365 offer retention for up to 365 days, lower-priced plans have shorter durations and no plans offer indefinite retention. Even in Microsoft's world, longer retention timeframes requires pushing audit log entries to another system.

### GROUP SPRAWL

Group sprawl – the tendency for the number of groups to increase at a rapid pace, some of which may no longer be necessary – is an increasing issue in Office 365, particularly with the popularity of Microsoft Teams. This is occurring because, by default, anyone in your organization can create Office 365 Groups, and it turns out that many users unfamiliar with Office 365 provision groups accidentally. This is a serious issue in the context of information governance, since it can lead to data management problems, such as data fragmentation. Given that group sprawl can happen both intentionally and accidentally, it creates a situation in which more and more server space is consumed and data becomes harder to find and manage.

### EVENTS IN THE AUDIT LOG

As a vital provider of insight into what is happening across the organization's digital footprint, audit logging should include:

- A complete set of relevant events from on-premises and cloud-based solutions. Office 365's audit log contains many events generated in Office 365, but excludes mail flow events in Exchange Online, event logging from on-premises solutions, and event logging from other cloud-based solutions. The Office 365 audit log provides partial insight only.

- Some audit events - or periods of time for all audit events - will contain important signals for legal cases, such as whether someone did or did not perform an action in Office 365. Being able to place audit events on litigation hold ensures appropriate evidence is retained, but this capability is not offered in Office 365.

- When audit log events are exported for analysis in other tools, such as Microsoft Excel, there should be no limit on the number of events that can be exported at any time. Office 365 imposes an artificial limit of 50,000 events per export.

- Audit events should be logged and available for review in as near real-time as possible. Some workloads in Office 365 log in near real-time (hat tip, Exchange Online), while other newer workloads – such as Microsoft Teams – can take up to 24-hours to push events to the audit log. Such a delay is inexcusable.

- Immutable storage of audit log events should be available, to guarantee log events were not modified or deleted after being created. Office 365 does not offer such capabilities; a third-party solution is required for situations where immutable storage is necessary.

***When audit log events are exported for analysis in other tools…there should be no limit on the number of events that can be exported at any time.***

### SUPERVISORY REVIEW CAPABILITIES

Supervisory review capabilities received their start in the financial services industry, via industry regulations requiring human oversight and supervision of communications to ensure rogue actors were not engaging in unethical behaviors. For organizations subject to such regulations, having an effective way of reviewing specific communication types is essential. Required capabilities include:

- Broad availability across Office 365 plans and non-Office 365 data repositories, in order to provide a broad picture of all communications and sampling at a pre-defined rate for supervision. Supervisory review capabilities in Office 365 are only available in the higher-priced Office 365 plans, and only apply to email messages, Microsoft Teams chat and channel messages stored in Exchange, and any third-party data imported into Office 365 and converted into an Exchange email format. They do not support other communication forms in SharePoint and Yammer that are not stored in Exchange Online. Note that content from Microsoft Teams faces a delay of up to 24 hours before being available for supervisory review, and the ability to sample third-party content depends on the frequency of import.

- Case management and workflow tools for managing supervised content, including escalation and discussion between multiple supervisors. These capabilities have been signaled as on the roadmap for supervisory review in Office 365, but are currently unavailable. This means supervisors must escalate and discuss specific content items using tools outside of the supervision toolkit.

- Logging of additions and changes to supervision policies to create an enduring record of who created, modified or deleted a policy at a specific point in time, in order to give evidence of compliance with supervision regulations. The Office 365 audit log is blind to supervision policies. Creating, editing, and deleting supervision policies are not audit logged.

- Unified visibility for supervisors across all of the supervision policies they have access to. Office 365 provides access to policy matches on a policy-by-policy basis, meaning that if a supervisor is overseeing five different policies, he or she must visit each in turn to review matches and decide whether any captured messages are valid or questionable.

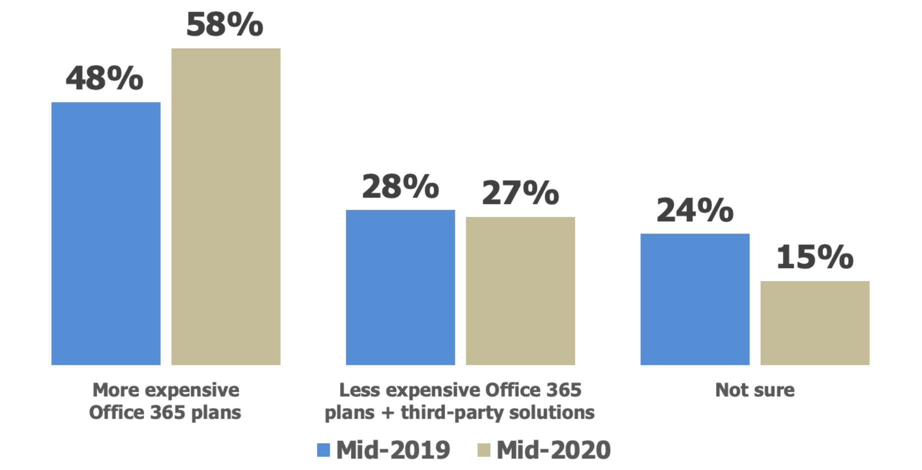
While supervisory review had its start in the financial services industry, be aware that Microsoft is attempting to extend its remit for additional scenarios beyond compliance, such as capturing and reporting on instances of offensive language. And despite the additional scenarios, the core ability to review communications between people can have relevance for any organization wanting to be proactive in minimizing deliberate or obfuscated wrongdoing.

***While supervisory review had its start in the financial services industry, be aware that Microsoft is attempting to extend its remit for additional scenarios beyond compliance.***

## Comparing the Costs

Microsoft offers a large number of SKUs for Office 365 covering a wide range of price points, although our research has found that the most commonly deployed plans for business customers are Enterprise Plans E3 and E5. While Plan E5 provides the full array of security, archiving and other capabilities available in Office 365, it is possible to employ Plan E3 (with a retail price that is 43 percent lower than Plan E5) in combination with third-party solutions that will either supplement or replace some of the native capabilities in Office 365. Current and anticipated preferences for the use of native vs. third-party solutions in Office 365 are shown in Figure 3.

**Figure 3**
**Preferences for Use of Native vs. Third-Party Solutions in Office 365**
Percentage of Organizations, Mid-2019 and Mid-2020



*Source: Osterman Research, Inc.*

As examples, we compared two sets of solutions that can be used in combination with Office 365 Plan E3:

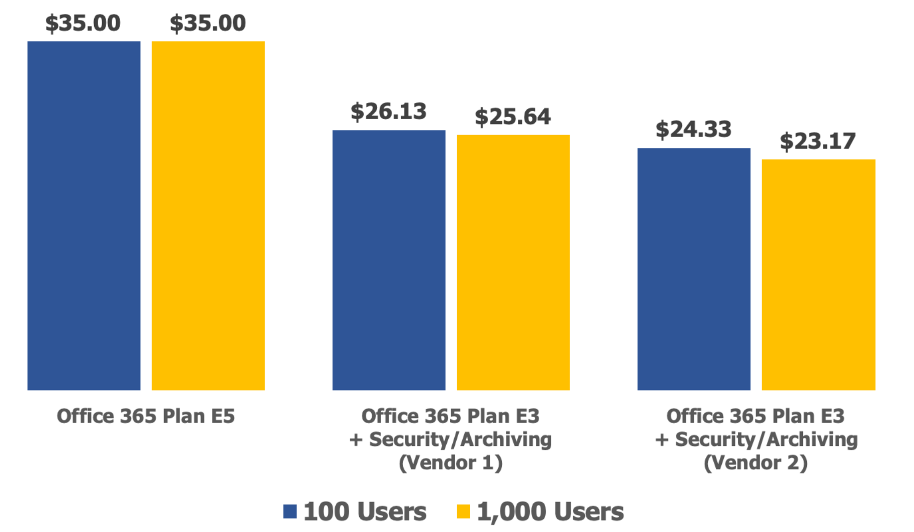
- Vendor 1: US-based provider of security and archiving capabilities
- Vendor 2: European provider of security and archiving capabilities

Based on the list prices that are publicly available for Office 365 Plans E3 and E5 and for the solutions shown above, Figure 4 shows the comparison of the various solutions. As shown in the figure, the total cost of purchasing Plan E3 in combination with third-party solutions is anywhere from 25 percent to 34 percent less expensive than the cost of a subscription to Plan E5.

It's important to note that Plan E5 offers some capabilities that are not duplicated completely with a combination of Plan E3 and third-party solutions, but the vast majority of business-grade requirements will be satisfied using the latter.

***For the majority of Office 365 users, we believe that a combination of Plan E3 and various third-party solutions will offer what most users need.***

**Figure 4**
**Comparison of Office 365 Plan E5 and Plan E3 with Third-Party Solutions**
Cost per month per user (US dollars)



*Source: Osterman Research, Inc.*

### THE BOTTOM LINE ON COSTS

Osterman Research believes that Plan E5 offers a number of useful capabilities and, for some users, the 75 percent premium that Microsoft charges for it over Plan E3 will be worth it. However, for the majority of Office 365 users, we believe that a combination of Plan E3 and various third-party solutions will offer what most users need, but at significantly lower cost. For example, a 100-user organization will save $10,644 to $12,800 per year by using Plan E3 and third-party solutions; an organization of 1,000 users will save $112,320 to $142,000 per year.

*Plan E3 – in combination with third-party solutions – is anywhere from 25 percent to 34 percent less expensive than Plan E5.*

## Summary

We encourage you to make use of Office 365 for productivity and team collaboration if it meets your business needs in these areas and aligns with your IT strategy. It is a widely used platform, and has a great deal of market momentum behind it.

However, be aware that in security and compliance areas more focused third-party providers are likely to offer better capabilities than relying solely on what Microsoft has to offer, and for organizations who use non-Microsoft tools and on-premises solutions in addition to Office 365, third-party solutions will certainly be the better route.

Part of the due diligence process in evaluating Office 365 as a decision maker is to decide what are essential capabilities and priorities for your organization, and whether the capabilities on offer in Office 365 meet or exceed these, or if a third-party solution better complements Office 365 and offers a better approach, given your needs.

# Sponsor of This White Paper

Conquer the challenges of Office 365 with Quest®, your go-to for moving, managing and securing Azure AD, Exchange Online, OneDrive for Business, SharePoint Online and Teams. Only with Quest will you get the most comprehensive set of Office 365 and hybrid management solutions, which now include the products from Metalogix, the leaders in SharePoint and OneDrive.

- **Pre-migration readiness**: Clean up and optimize your environment with pre-migration planning, thorough assessments and remediation to speed up your migration and reduce Office 365 licensing costs.
- **ZeroIMPACT migration**: Minimize risk and business disruption by ensuring a ZeroIMPACT Office 365 migration or tenant-to-tenant consolidation for your entire organization.
  - Migrate to Exchange Online from on-premises Exchange mailboxes and public folders, Outlook PSTs, third-party email archives, Google Gmail, and IBM Lotus Notes.
  - Migrate SharePoint content, lists, user permissions and Lotus Notes applications to SharePoint Online.
  - Move to OneDrive for Business from local file shares, Google Drive, Box and Dropbox
- **Continuous security and compliance**: Use automation (versus PowerShell) to simplify Office 365 management and security tasks, reducing risk and complexity.
- **Administration automation**: Manage your cloud or hybrid environment with ease using automated Quest solutions for user lifecycle management and provisioning, backup and recovery and license reporting.

Quest

**www.quest.com**

**@Quest**

**+1 800 306 9329**

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.