WHITE PAPER

The Need for Third-Party Security, Compliance and Other Capabilities in Microsoft® Office 365®

An Osterman Research White Paper

Published July 2013

McAfee®
An Intel Company

OSTERMANRESEARCH

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

Microsoft Office 365 is a leading, cloud-based solution from the world's largest software company. It offers email, instant messaging, telephony, content management, desktop productivity, security, archiving and other capabilities delivered from Microsoft's worldwide network of cloud data centers. It is offered in a large (some would say confusing) number of versions at price points ranging from free to $20+ per user per month.

While Office 365 is, to some extent, marketed as something of a "one-stop-shop" for communication and collaboration needs, it is a generalist product by its very nature, as are all cloud-based communication and collaboration tools offered to a mass audience. In short, Office 365 cannot satisfy every requirement for every user at every organization. Consequently, Osterman Research believes that most mid-sized and large organizations (as well as many smaller ones) that are considering Office 365 will need to use third party offerings that will supplement the capabilities in Microsoft's offering or that will serve as replacements for them.

KEY TAKEAWAYS

- Office 365 is a good platform for communications and collaboration and offers robust functionality with reasonable reliability.
- There are limitations in Office 365 – particularly with regard to security and archiving – that many organizations will want to layer or replace with third party solutions that will better satisfy their particular requirements.
- Although Office 365 is a cloud-based solution, some of the more advanced capabilities of Office 365 require a significant level of on-premises infrastructure or the use of third-party capabilities.
- The majority of mid-sized and large organizations will deploy Office 365 using a hybrid model of cloud-based and on-premises infrastructure because of their inability or the cost effectiveness of migrating all capabilities to the cloud.

The majority of mid-sized and large organizations will deploy Office 365 using a hybrid model.

A CAVEAT

The goal of this white paper is not to denigrate Office 365, its capabilities or Microsoft. In fact, we believe Office 365 is quite robust and useful for a large number of organizations. However, our goal is to be as honest and balanced as possible in discussing both the advantages and drawbacks of Office 365. As with any cloud-based communications and collaboration tool, there are limitations in Office 365 that can be satisfied through the use of third party tools and services. Any limitations discussed here are not limited to Office 365, but can be part of any cloud-based solution.

ABOUT THIS WHITE PAPER

Osterman Research conducted a market research survey with organizations that had at least 50 email users and that had not definitely ruled out the possible use of Office 365. In fact, 5% of the email users in the organizations surveyed are currently served by Office 365, a figure that is expected to increase to 22% by May 2014.

The survey, conducted in early May 2013 with the Osterman Research survey panel, focused on capabilities, features and functions that these organizations would require from their communication and collaboration systems, and how well these might be satisfied by Office 365 and other solutions. Some of the results from that survey are discussed in this white paper, but a separate document will be made available specifically focused on all of the survey results.

The sponsor of this white paper is McAfee. Information about the company and its relevant offerings are included at the end of this paper.

WHY ARE ORGANIZATIONS USING OFFICE 365?

CORE FEATURES AND OVERVIEW OF THE PLATFORM

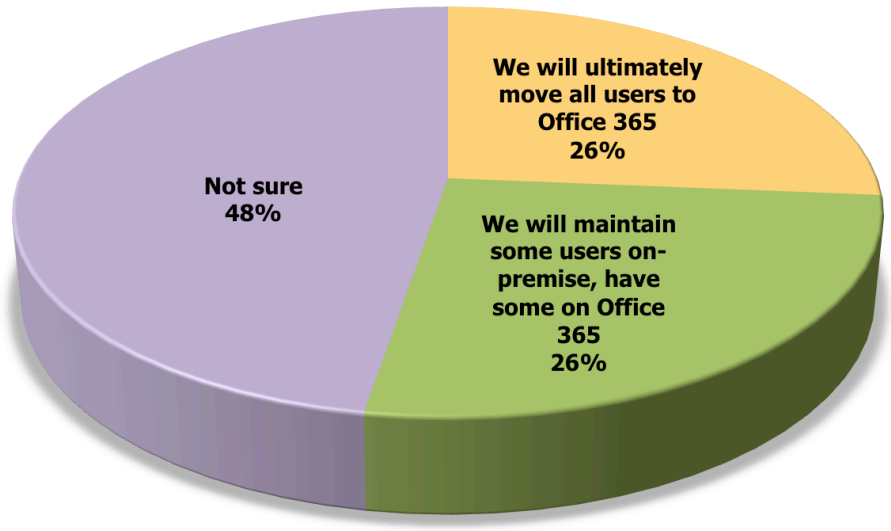
Office 365 is a collection of cloud-based offerings that includes Exchange Online (most accounts offer 25-gigabyte mailboxes), SharePoint Online, Lync Online and Web-based versions of desktop productivity applications, as shown in the table on the next page. Organizational decision makers are seriously considering the use of Office 365 and other cloud-based messaging and application platforms because they can offer lower and more predictable costs of ownership, the ability to free IT staff for other tasks, and to add new capabilities that would either require the addition of new staff members or access to expertise that is not readily available. Our survey found that an important or extremely important reason for migrating to Office 365 is to reduce email costs (cited by 66% of decision makers and influencers), to reduce the workload for IT staff (61%), and to free up IT staff for other projects or initiatives (55%).

INCREASING USE OF OFFICE 365

In April 2013, Microsoft claimed that 25% of enterprises (defined by Microsoft as organizations with at least 250 employees instead of the more commonly accepted standard of 1,000+ employees[i]) are now using Office 365 and that the service is now running at a rate of generating $1 billion in annual revenues[ii]. While the former claim means that 25% of enterprises have Office 365 running within them for at least *some* of their users, there is no doubt that the platform is becoming more popular as decision makers consider increased use of cloud email and related services. In fact, as shown in the following figure, one in four organizations surveyed by Osterman Research that have not ruled out the use of Office 365 anticipate that they will move all of their users to the platform at some point. However, an equal number believe they will use a hybrid model of Office 365 and on-premises infrastructure. Osterman Research believes that the hybrid model will ultimately be the most commonly used model for deploying Office 365 in mid-sized and large organizations.

Plans for Migrating to Office 365

Among organizations that are still considering a migration to Office 365



DIFFERENCES BETWEEN OFFICE 365 AND BPOS

Microsoft BPOS, the predecessor to Office 365, was introduced in late 2008 and was quite successful, selling several million seats. At the same time, BPOS was controversial with Microsoft's significant ecosystem of hosted Exchange providers

Our survey found that an important or extremely important reason for migrating to Office 365 is to reduce email costs, to reduce the workload for IT staff, and to free up IT staff for other projects or initiatives.

because Microsoft's per-seat pricing for BPOS was much lower than many providers' pricing for hosted Exchange.

Moreover, BPOS was built on the 2007 versions of Exchange, SharePoint and Office Communications Server (now Lync Server) instead of the more cloud-friendly 2013 versions on which Office 365 is based. Plus, while BPOS was designed for smaller businesses, Office 365 was designed for enterprises, as well, a market into which Microsoft has been making significant inroads.

Selected Versions and Costs for Office 365

Version	Includes	$/User/ Month
Exchange Online Plan 1	Hosted Exchange, spam and malware filtering, Active Integration, In-Place Archive	$4.00
Exchange Online Plan 2	Same as above plus In-Place Hold, unlimited storage, hosted voicemail and DLP[iii] capabilities	$8.00
Office 365 Enterprise E1[iv]	Hosted email with 25Gb of storage, plus Office Web apps, basic file sharing, Web conferencing, public Web site, intranet capabilities, etc.	$8.00
Office 365 Enterprise E3	Same as above plus desktop versions of Microsoft Office, Office Mobile apps, email archiving and legal hold capabilities, unlimited archival storage, eDiscovery Center (supports Exchange, SharePoint and Lync), hosted voicemail, business intelligence	$20.00
Office 365 Enterprise E4	Same as above plus enterprise voice, business intelligence tools	$22.00
SharePoint Online Plan 1	App catalog and marketplace, team sites, work management, social capabilities, external sharing, basic search, standard search, content management, records management, access services, SharePoint 2013 workflow	$3.00
SharePoint Online Plan 2	Same as above plus enterprise search, e-discovery, ACM, compliance with various regulatory requirements, Excel services, Visio services, form-based applications, business connectivity services	$7.00
Lync Online Plan 1	Presence, instant messaging, IM federation (w/Windows Live), Skype connectivity, Lync-to-Lync calling, Lync mobile clients	$2.00
Lync Online Plan 2	Same as above plus desktop, application and whiteboard sharing; multiparty content sharing, interoperability with third-party audio conferencing services, multi-party video, etc.	$5.50

In addition to the offerings noted above, there are a number of other Office 365 versions, including:

Business
- Office 365 Small Business (up to 25 users): $5.00/user/month
- Office 365 Small Business Premium (up to 25 users): $12.50/user/month
- Office 365 ProPlus: $15.00/user/month
- Office 365 Midsize Business (up to 300 users): $15.00/user/month

Education
- Office 365 Education A2: free to students and faculty/staff
- Office 365 Education A3: $2.50-4.50/user/month
- Office 365 Education A4: $3.00-6.00/user/month

Government
- Exchange Online Plan 1: $3.50/user/month
- Exchange Online Plan 2: $7.00/user/month
- Office 365 (Plan 1) for Government: $6.00/user/month
- Office 365 (Plan 3) for Government: $17.00/user/month

Kiosk
- Exchange Online Kiosk: $2.00/user/month
- Office 365 K1: $4.00/user/month
- Office 365 K2: $8.00/user/month

By just about any measure, Office 365 is a very solid offering from a leading and well-respected vendor. While Microsoft has been offering cloud-based email for many years, the current versions of their cloud offerings are robust and offer enterprise-grade features and functions. Moreover, Microsoft has made Office 365 compatible with a range of key standards and other requirements as verified by various third parties[v], further enhancing its appeal for enterprise customers:

- Business Associate Agreements under the Health Insurance Portability and Accountability Act (HIPAA)
- The Federal Information Security Management Act (FISMA)
- International Organization for Standardization (ISO) 27001
- European Union (EU) Safe Harbor and Data Protection Directive Model Clauses
- The Gramm-Leach-Bliley Act (GLBA)
- The Family Educational Rights and Privacy Act (FERPA)
- Title 21 CFR Part 11 of the Code of Federal Regulations
- The Federal Information Processing Standard (FIPS) 140-2
- Trusted Internet Connections (TIC)

What this means is that Office 365 may be used in a variety of regulated environments, such as healthcare, government and in the European Union. Microsoft also benefits from robust support for a hybrid model given its commanding market share for desktop productivity applications and its dominance in the business email market through Exchange.

By just about any measure, Office 365 is a very solid offering from a leading and well-respected vendor.

WHY ORGANIZATIONS MAY HESITATE TO USE OFFICE 365

In spite of Office 365's several benefits, it has some limitations that are worth noting:

SECURITY ISSUES

- No versions of Office 365 offer end user access to the spam quarantine for self-management capabilities[vi]. Exchange Online Plans 1 and 2 do not provide for administrator management of the quarantine[vii].
- Office 365 does not support operating redundant spam filters in parallel with Office 365's built-in spam protection.
- Office 365 does not include advanced and targeted threat protection techniques, such as real-time link following, to emulate the contents for malware, in addition to reputation checks.

- There is no support for blacklists in Office 365 P1.
- There is no support to take action on an email containing a link strictly based off the URL reputation alone.
- There is no support to help users on mobile devices determine whether a link in an email is safe to click on.
- Instant messaging and file filtering are not available with any Office 365 plans[viii].

ARCHIVING ISSUES

- Archiving in Office 365 has some limitations, including lack of support for Exchange Online archiving with Outlook 2011 under Mac OS X, as well as lack of support for accessing archived emails via Android and iPhone devices.
- Archiving for Lync Online does not include some types of Lync content, such as peer-to-peer file transfers, conferencing annotations, application-sharing for peer-to-peer instant messages and conferences, or audio/video for peer-to-peer instant messages and conferences. Moreover, archiving settings cannot be directly controlled from inside the Lync administration center, but instead are controlled by the Exchange mailbox In-Place Hold attribute established for each user's email account[ix]. Archiving of Lync content requires a legal hold to be placed on the mailbox. Moreover, Lync archiving can be accomplished only with the Lync desktop application and not at the server level, such as when users are logged into Office 365 via Web services.
- SharePoint Online, while offering eDiscovery, compliance with various regulatory obligations and other capabilities, does not archive content. Because of the growing amount of content that is stored in SharePoint-enabled organizations, the ability to archive this content is critical.
- The In-Place Archive (formerly known as the Personal Archive) is a secondary mailbox that can be deployed on the same or a different server from a user's primary mailbox. The In-Place Archive or retention policies require either an Exchange Server account or an Exchange Online account together with an Exchange Server Enterprise Client Access License and only certain Outlook licenses – a variety of Outlook versions are not supported[x].
- Office 365 requires an external mailbox or third party archive for journaling capabilities (journaling is the process of capturing a copy of emails that can then be archived). Our research found that 57% of the organizations we surveyed are interested or very interested in journaling for compliance purposes, making this capability more cumbersome to implement in many environments.
- Only Plans E3 and E4 offer unlimited storage (others must share the 25 Gb of space between the primary mailbox and the In-Place Archive).
- End user search capabilities in Office 365 are more limited than they are with many competing cloud-based and on-premises archiving solutions.
- There are no native surveillance features in Office 365 that allow monitoring or sampling of communications – this is an important capability for highly regulated firms, such as financial services firms that must sample communications per FINRA Regulatory Notice 07-59[xi].
- For organizations that need to journal content into Office 365 – such as Salesforce Chatter content, instant media, social posts, etc. – they will require the use of a third party archiving solution, since journaling within Office 365 does not support import of external, non-Lync content.

SharePoint Online, while offering eDiscovery, compliance and other capabilities, does not archive content. Because of the growing amount of content that is stored in SharePoint-enabled organizations, the ability to archive this content is critical.

PERFORMANCE ISSUES

- The maximum number of email messages that can be delivered is 30 per minute[xii].
- For messages sent to 5,000+ recipients, the maximum size of the message is two megabytes[xiii].
- The maximum number of POP or IMAP connections is 20 and the maximum number of concurrent Exchange ActiveSync connections is four[xiv].

RETENTION ISSUES

- Items in the Deleted Items and Junk E-Mail folders can be retained for a maximum of 30 days[xv].
- The maximum size of the arbitration mailbox is ten gigabytes[xvi].
- Office 365 Plans E3 and E4 can have the Recoverable Items Folder (formerly known as the Dumpster) set to retain deleted emails beyond the default 30 days to "any other value"[xvii] (dependent on the storage quota limitations for the Recoverable Items Folder). This capability is simply a hidden folder that allows users to recover email that was intentionally or mistakenly deleted. For SharePoint Online, data is backed up twice each day and retained for 14 days.

SHAREPOINT ISSUES

- SharePoint Online for Office 365 Enterprise, Education and Government is limited to[xviii]:
  - 500 megabytes per subscribed user (but additional storage is available for an additional fee).
  - The storage base per tenant is 10 gigabytes plus the limit noted above.
  - There can be no more than 100 gigabytes per site collection.
  - The file upload limit is 250 megabytes per file.
  - The maximum number of unique external users is 10,000 per month.
- The SharePoint Online API requires custom code to work with the Microsoft sandbox model.
- SSL is not available in SharePoint Online for some Office 365 users.

MOBILITY ISSUES

- Office 365 will wipe only those mobile devices that are managed using ActiveSync.
- BlackBerry Enterprise Server (BES) is not supported in Office 365. Despite declining support for BES in some organizations (a situation that we believe will be reversed over the next 24 months as BlackBerry regains lost market share), this is a serious problem for organizations that still have many BlackBerry users.
- Office on Demand, a key feature of Office 365 that permits temporary Office client to be installed on any Windows 7/8 PC, is not supported on the iPad, the most commonly deployed tablet computer in the workplace.

MAILBOX ISSUES

- Shared mailboxes in Office 365 are provided at no charge, but cannot be larger than five gigabytes and can be created only with Remote PowerShell. Moreover, a shared mailbox cannot be accessed by users of an Exchange Online Kiosk

Office on Demand, a key feature of Office 365 that permits temporary Office client to be installed on any Windows 7/8 PC, is not supported on the iPad.

license and cannot archive emails from individual users[xix].

- Inactive mailboxes (i.e., deleted mailboxes) can have their contents held indefinitely if an In-Place Hold is exercised before the mailbox is automatically deleted. While the contents of a deleted mailbox can be recovered for 30 days after deletion, both the mailbox and its contents will not be recoverable after 30 days if the hold is not activated[xx].

OS AND APPPLICATION VERSION ISSUES

- Windows XP/SP3 and Vista SP2 will not be supported after 2013[xxi].

- Outlook versions earlier than 2007 (Windows) or 2011 (Mac) with all patches and service pack upgrades are the minimum versions supported with Office 365[xxii].

DATA LOCATION ISSUES

- Microsoft stores Office 365 customer data in various countries based on the location of the customer[xxiii], can move customer data without notice, and will not guarantee exactly where a customer's data will be stored. For example:
    - North American customers: primary data centers are located in the United States.
    - Government customers in the United States: primary data and backup centers are located in the United States.
    - Most EMEA customers: primary data centers for Office 365 are in Ireland and the Netherlands; Lync Online customers provisioned before October 2011 may be hosted from a US data center.
    - Asia Pacific customers: the primary data centers for Office 365 data are in Singapore and Hong Kong, but a data center in Ireland is used for Active Directory and Global Address Book data. Lync Online and Online Portal data are served from a US data center.
    - South American customers (except Brazil): primary data centers are located in the United States.
    - Brazilian customers: the primary data center for SharePoint Online is in Brazil; for Exchange Online customers after October 30, 2011, a Brazilian and US data are used interchangeably as the primary data centers; for Exchange Online customer provisioned before October 30, 2011, the primary data center is in the United States.
    - Microsoft states that it "uses one or more of its data centers in the United States as the backup data center for all services" for US and South American customers. Backup data centers for EMEA customers are in Ireland and the Netherlands, except that Active Directory and Global Address Book data are hosted in US data centers for performance reasons. For Asia Pacific customers, backup data centers are used in Singapore and Hong Kong, but a data center in Ireland is used for backup of Lync Online Active Directory, Global Address Book data and Online Portal.

OTHER ISSUES

- Users of Office 365 do not necessarily control when they will be upgraded, since Microsoft determines when upgrades occur[xxiv].

- Backup and recovery of customer data are controlled only by Microsoft.

- Although Office 365 proposes a utility-based model for licensing, automatic plan assignment or re-assignment as a user changes roles is not available through

Users of Office 365 do not necessarily control when they will be upgraded, since Microsoft determines when upgrades occur.

DirSync/ADFS, as is also the case for true single sign-on capability. Cloud-based, third party solutions can help to fill this gap.

- Single sign-on supported in Office 365, but only with Active Directory Federation Services.

- With an Exchange Server on-premises, admins can access log files using simple scripting, a feature not possible in Office 365.

THE NEED FOR BETTER SECURITY IN OFFICE 365

Microsoft offers a number of security capabilities in Office 365: anti-virus and anti-spam filtering; physical access controls that using multiple authentication schemes at its data centers that are managed by Microsoft Global Foundation Services; and employee access that is restricted by job function; among other capabilities. However, there are some security issues that decision makers should take into account as they consider a move to Office 365, including:

- **Office 365 uses a multi-tenant architecture**
  The Office 365 architecture is multi-tenant, meaning that multiple customers' environments run on the same servers. While this *can* be a secure environment, many organizations – particularly those in highly regulated industries or those with very sensitive information – may not be comfortable in such a shared data environment. Despite the fact that Microsoft isolates customer data into silos, the company offers the ability to store Office 365 data on dedicated hardware for an additional cost[xxv].

- **Extra security layers may be needed**
  Microsoft Exchange Online Protection (EOP)[xxvi] uses multiple scanning engines from leading security vendors and EOP's SLA claims to detect 100% of all *known* viruses with updates every 15 minutes. That said, some customers may want to add an additional layer of inbound protection/detection for increased abilities for phishing or spearphishing detection capability, for example. Or they may simply want to add another layer of malware or spam filtering for additional protection. For example our research found that the potential market for Office 365 finds the following email protection capabilities to be important or very important, capabilities that may not be fully satisfied by an Office 365-only deployment:

  - Cloud email providers offering SLAs for spam and malware filtering (65%)
  - The availability of multiple malware scanners for incoming email (62%)
  - Multi-vendor threat protection (62%)
  - Integrated, end-to-end encryption (58%)
  - "Graymail" filtering capabilities (42%)
  - Integrated DLP for scanning the email channel (50%)

  Graymail capabilities have been added to EOP, but the system classifies graymail as spam, leaving it undifferentiated from actual spam. DLP compliance template capabilities have also been added to EOP, but they will not satisfy all customers' requirements. Plus, Lync Online does not scan files or other content for malware, nor does it archive instant messaging content as noted above. Moreover, it is essential to segment phishing content from spam, allowing for proper management of phishing messages (e.g., not placing phishing messages in the same quarantine as spam so that end users are prevented from opening phishing messages and having their PC and network potentially compromised).

- **Filtering limitations**
  While most versions of Office 365 provide reports of received or sent spam, and malware detections in received or send email, Office 365 Small Business and

The Office 365 architecture is multi-tenant, meaning that multiple customers' environments run on the same servers.

Office 365 Small business Premium do not.

- **Advanced threat protection**
  Office 365 may not provide the level of protection from advanced threats that many organizations will require. For example, if an attacker creates a new URL specifically targeted against a company and links it to malware, EOP may not scan those new links and the content behind those links at the time of click to block those that are malicious. Because many larger organizations will need to wrap advanced security capabilities like these around Office 365, the base security capabilities in Office 365 will need to be carefully evaluated in light of decision makers' attitudes toward risk.

- **Mobility limitations**
  Office 365 wipes only ActiveSync devices, which can be a major limitation in the large number of organizations that still support BlackBerry devices and do not want to do via ActiveSync. Moreover, while all versions of Office 365 support BlackBerry Internet Service, not all versions support BlackBerry Business Cloud Services. Although BlackBerry supports ActiveSync, some have reported problems in doing so. An alternative for many organizations will be to deploy BlackBerry Enterprise Services, which will offer support for not only BlackBerry devices, but also iOS and Android devices.

- **Microsoft manages Office 365 backup and recovery**
  Microsoft manages all of the backup and recovery of content for Office 365 customers unless customers have implemented their own capabilities at an additional cost, nor are there native selective restore capabilities. While Microsoft managing backup and recovery is not an inherent weakness per se, customers must rely on Microsoft to manage these aspects of the Office 365 experience and to do so in a timely manner. Plus, as noted above, Microsoft determines where it stores customer data, which can be a problem for many customers in jurisdictions with strict privacy requirements and restrictions on the geographic location of data.

- **Single sign-on capabilities can be very complex**
  Single sign-on (SSO) capabilities are supported in Office 365, but they can be complex. For example, the use of the Microsoft Online Services Sign-In Assistant that can streamline authentication for client applications is not an actual SSO capability because it actually combines two passwords[xxvii]. True SSO is achievable with Office 365, but only when Active Directory Federation Services (ADFS) are used in networks that are running Windows Server 2008 Active Directory on-premises. This means that in an enterprise environment, a fair amount of on-premises infrastructure will still be required in order to effectively manage Office 365 access.

- **The Office 365 SLA may not be adequate**
  While Microsoft offers an SLA for Office 365[xxviii], it is important to note that it may not be as robust as some decision makers might like. For example:

  - "Service Credits are Customer's sole and exclusive financial remedy for any violation of [the Office 365] SLA."

  - "The Service Credits awarded in any calendar month shall not, under any circumstance, exceed Customer's monthly service fees."

  - The service credits equal 25% of the service fee only if monthly uptime drops below 99.9% (43 minutes per month), 50% if monthly uptime drops below 99% (seven hours 12 minutes per month), and 100% if monthly uptime drops below 95% (36 hours per month).

  - The SLA does not apply "to factors outside Microsoft's reasonable control", "that resulted from Customer's or third-party hardware or software", "during

While Microsoft offers an SLA for Office 365, it is important to note that it may not be as robust as some decision makers might like.

scheduled downtime", or "during beta and trial services (as determined by Microsoft)".

Microsoft calculates "monthly uptime" in such a way that high levels of downtime could be experienced by some Office 365 users without triggering the payment of Service Credits. For example, consider the case of a 1,000-user organization with 800 users in North America and 200 users in Europe. If the European customers experienced three hours of unplanned downtime in one month and 30 minutes of downtime as a result of scheduled maintenance, but the North American users experienced no downtime during that month, Microsoft would calculate total uptime for that month across the entire organization at 99.92%. This means that although the European users experienced uptime of only 99.51% during that month, no Service Credits would be paid.

The bottom line is that Office 365's included security is a reasonably solid offering, but it does not offer the advanced protection level of a pure play security provider and, therefore, may not be the most suitable security solution for every organization.

THE NEED FOR BETTER COMPLIANCE IN OFFICE 365

Another one of the key issues that Osterman Research has discovered in its research over the past several years is that many decision makers do not consider their specific archiving, security and compliance requirements in as much detail as they should. Moreover, many do not consider all of their long-term archiving and compliance requirements before migrating to a cloud-based messaging platform. However, when migrating to the cloud, a new set of compliance considerations becomes important to understand before any decisions are made.

Office 365's included security is a reasonably solid offering, but it does not offer the advanced protection level of a pure play security provider.

BETTER ARCHIVING CAPABILITIES

Many organizations have a regulatory obligation to retain various types of data and ensure its authenticity and integrity for many years, in some cases indefinitely. The In-Place Archives in Office 365 do not address these types of requirements as well as some third party archiving solutions, since users can delete content from the former.

Only Office 365 Plans Enterprise E3 and E4 offer unlimited archive storage quotas and litigation hold capabilities, meaning that users not provisioned with these more expensive Office 365 plans may require additional archiving capabilities to ensure adequate retention of their data. Moreover, the other plans share storage between the primary mailbox and the archive, whereas the E3 and E4 plans do not.

Our research found that 50% of those surveyed consider third party backup and archiving capabilities for Office 365 to be important or very important – 40% of respondents consider third party backup and archiving for SharePoint data to be this important. This means that a sizeable proportion of the Office 365 market will want to deploy additional backup and archiving capabilities, negating some of the cost advantage of migrating to Office 365.

While placing a mailbox on litigation hold in Office 365 or journaling prevents users from deleting messages, the Messaging Records Management (MRM) capability in Office 365 or Exchange Online does not. For example, Microsoft states that "MRM doesn't guarantee retention of every message. For example, a user can delete or remove a message from their mailbox before the message reaches its retention age; MRM isn't designed to prevent users from deleting their own messages."[xxix] This means that some organizations with strict requirements for retaining all relevant messages, such as financial services companies, may need to seek alternative archiving solutions that will ensure retention of all messaging content.

GEOGRAPHIC AND JURISDICTIONAL REQUIREMENTS

Some organizations are under strict obligations to comply with various jurisdictional requirements, such as a requirement that data not leave a particular geographic area or that it not be moved to a nation that does not offer adequate protection of sensitive data. However, Microsoft admitted in June 2011 that content in its data centers can be handed over to US or other authorities and that customers might not be notified of this disclosure[xxx]. Moreover, as noted above, customer data can be moved to a variety of locations for day-to-day management or backup purposes. On the other hand, some third-party archiving solutions offer more transparency about where customer data resides, which will alleviate some decision makers' concerns. This is particularly true for non-US customers that may not want their data subject to review under the PATRIOT Act, by the IRS[xxxi] or other US government agencies.

Another consideration, not only for Office 365 but for all could providers in general, is the issue of blind subpoenas – subpoenas issued by a government authority without the knowledge of the customer. Because a cloud provider can be compelled to grant the government access to customer records without informing their customer of the activity, some organizations may decide that on-premises archiving of cloud-based content is preferable.

CONTENT AVAILABILITY

An important limitation of Office 365 is that if the service experiences a downtime incident, the archived content is also unavailable. Use of a third party archiving solution eliminates this limitation by storing data in two different infrastructures, allowing users to access their archived content and, as part of a business continuity solution, to send and receive emails while Office 365 is unavailable. This is not a trivial consideration, since there have been some serious outages in the Office 365 infrastructure. For example, in January 2013 alone, there were four major outages that affected Microsoft's online services.

DLP

Microsoft has implemented DLP in Office 365, Exchange Online and Exchange 2013 based on Exchange Transport Rules[xxxii]. Through the use of Policy Tip notification messages, Outlook users can be alerted to potential violations of corporate policies when sending email that might contain sensitive or confidential information[xxxiii]. Microsoft has provided a number of definitions[xxxiv] that can be used out of the box, but allows admins to create custom definitions, as well.

As of this writing, DLP can be used only with Outlook 2013 for Policy Tips, not with Outlook Web Access when used with either Office 365 or on-premises Exchange. While DLP policies work for emails sent from other clients, the Policy Tips feature works only with Outlook 2013. Advanced capabilities such as file fingerprinting are also not available.

eDISCOVERY AND LITIGATION HOLD CAPABILITIES

The Enterprise plans for Office 365 provide built-in eDiscovery capabilities, but some organizations will need more sophisticated and granular functionality, such as highly configurable legal holds and robust case management when performing online reviews. Some organizations that have sophisticated eDiscovery requirements will find that although useful, Office 365's built-in capabilities might not meet their needs.

Several third-party archiving solutions offer more granular capabilities than are available with Microsoft's solutions, such as tamper-proof storage across all Office 365 plans, the ability to perform very complex searches for eDiscovery or regulatory compliance purposes, output to various file formats when exporting content to third-party review tools, and better support for EDRM requirements.

Important limitations in Office 365 in the context of eDiscovery include:

Several third-party archiving solutions offer more granular capabilities than are available with Microsoft's solutions.

- The In-Place Hold feature does not capture distribution list membership or BCCs, and so does not offer a complete record of every message sender and recipient.

- If an employee leaves the organization, his or her mailbox will be permanently deleted if not placed on hold within 30 days of its deactivation.

- Reviewing the data that results from a search can be more difficult in Office 365 than with some other tools. Because search results are copied to a discovery mailbox and then accessed via Outlook or OWA, this can make the review of large search results or sharing the responsibility of reviewing content across groups more time consuming. The lack of sophisticated review tools is a key consideration for organizations that need to perform early case assessment or similar types of operations across the entire organization[xxxv].

- The In-Place eDiscovery and Hold interface in Exchange Online can be used to implement an In-Place Hold for a maximum of only 50 mailboxes in a single search. If content needs to be captured for more than 50 mailboxes, the process must be repeated and content held in batches of 50 mailboxes, or IT must use the Exchange Management Shell command-line interface to manage discovery[xxxvi].

- If the eDiscovery Center in SharePoint Online is used, a search query across a maximum of 1,500 mailboxes is possible, but if more mailboxes must be searched multiple search queries must be run or the Exchange Management Shell command-line interface must be used[xxxvii].

- For Office 365 dedicated plans, a maximum of 15% of the mailboxes in Office 365 can be placed on hold at any given time. Once the maximum is reached, new mailboxes cannot be placed on hold[xxxviii].

NOT ALL PLATFORMS AND CONTENT SOURCES ARE SUPPORTED

Many organizations operate multiple on-premises and cloud-based platforms, and so will need an archiving and compliance solution that can support all of these platforms. Microsoft's archiving solutions do not currently support all of the platforms that an organization might have in place, such as competing mail systems like GroupWise, Notes/Domino or Google Apps; or various document repositories like Box or Dropbox. For example, while Microsoft offers online archiving for Exchange, it does not do so for SharePoint, requiring the use of a third party solution for organizations that need to archive SharePoint content.

This is an important consideration, since an eDiscovery effort, for example, can be made more complicated if an organization must extract content from multiple archiving systems – e.g., one for Office 365, one for SharePoint content, one for files, etc. Having a single archiving solution for all content streamlines eDiscovery, litigation holds and other activities.

STORAGE LIMITATIONS

Many organizations store very large amounts of information as a result of either long retention periods for email and other content, or because they preserve data-intensive files like engineering, graphic or architectural drawings. As a result, for some customers the limitations in Office 365's archiving for the less expensive plans will not be acceptable.

Many organizations operate multiple on-premises and cloud-based platforms, and so will need an archiving and compliance solution that can support all of these platforms.

ADDITIONAL ISSUES THAT DECISION MAKERS SHOULD CONSIDER

Decision makers will also need to answer four basic questions when decision on whether or not to migrate some or all of their users to Office 365 (or any cloud-based messaging and application platform):

1. Should we migrate our active mailboxes to Office 365?

2. Should we port our existing email archive to Office 365?

3. If yes to either, should we use Microsoft or a third-party to provide Office 365 services?

4. Should we use one or more other third parties to strengthen or provide other capabilities?

Here are some of the more important questions that decision makers should ask internally, of consultants and of vendors as they consider a possible migration to Office 365:

EMAIL-GENERATING APPLICATIONS

- What legacy applications are currently employed that will need to be rewritten, applications that cannot be migrated to the cloud because of regulatory or other considerations, or that will require on-premise infrastructure to support? Our research found that 36% of the organizations surveyed have more than 50 email-generating applications in place.

REGULATORY ISSUES

- To what extent do we or will we need to comply with SEC/FINRA, HIPAA, FERPA, SOX, GLBA and other regulatory requirements?

- How well will native Office 365 capabilities comply with our requirements and what are the holes we will need to fill with third party services?

- Will the native Office 365 DLP capabilities be sufficient to meet our compliance obligations and how well will they integrate with other DLP capabilities we might have today or in the future?

BUSINESS ISSUES

- Should third-party cloud vendors be used to enhance the security of Office 365, including vendors of email security, email encryption, business and compliance email archiving or Web filtering? For example, the Microsoft encryption solution is passive and can create problems from a risk management perspective.

- Migrating key services like email and collaboration to the cloud carries with it some level of risk, so should we employ multiple providers in order to distribute the risk? For example, if we are concerned about going "all-in" with a cloud strategy, will we be better off using a third-party archiving solution that will maintain copies of data at the Office 365 provider's and the archiving provider's data centers?

- Should we deploy Office 365 using only basic services with supplemental capabilities offered by third parties, or should we opt for more sophisticated (and more expensive) services initially, keeping in mind the limitations in migrating from less capable to more capable plans?

- Is the email security protection offered sufficient for the needs of our business, or should we be concerned about the risk of targeted attacks and layer an advanced cloud email security service around Office 365?

How well will native Office 365 capabilities comply with our requirements and what are the holes we will need to fill with third party services?

- What are the options available for cloud service portability? In other words, how easy or difficult will it be to migrate to Office 365, from Office 365 to another provider, or back to an on-premise service model?
- What is the *current* level of internal IT support that we could devote to managing the migration to and support for Office 365 and third-party offerings?
- What is the *desired* level of internal IT support for managing the migration to and support for Office 365 and third-party offerings?
- How will our organization respond and stay productive in the event of an Office 365 service disruption or outage?

ARCHIVING AND CONTENT MANAGEMENT

- Do we need redundant copies of our archived data in multiple locations?
- If yes, why? For data protection? Business continuity? Disaster recovery? What is the relative importance of each?
- Do we need to specify in which country(ies) our content will be stored?
- What will be the impact of the US PATRIOT Act on our ability to protect information?
- Do we need to add our corporate domain(s) and set up journal rules to capture all messages sent or received from Exchange Online directly within the administration console?
- What options are available for maintaining an on-premise archive of cloud-based content?

SERVICE LEVELS

- Is Office 365 able to meet our requirements for uptime/availability?
- How reliable are third-party solutions focused on security, encryption, archiving, compliance, etc.?
- What compensation is offered by providers following outages?
- What should our backup strategy for Office 365 data be?
- What metrics do we need to establish with regard to Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)?

MIGRATION SERVICES

- What services are offered for migrating existing, on-premise Exchange mailboxes and email security settings to Office 365?
- What services are offered for migrating from SharePoint to Office 365?
- What services are offered for migrating archived data from on-premise archiving solutions to either Exchange Online Archiving or a third party, cloud-based archiving solution?
- Do these services include mail route control, split domains or blended solutions that can streamline the migration process?
- To what extent are customization services required?

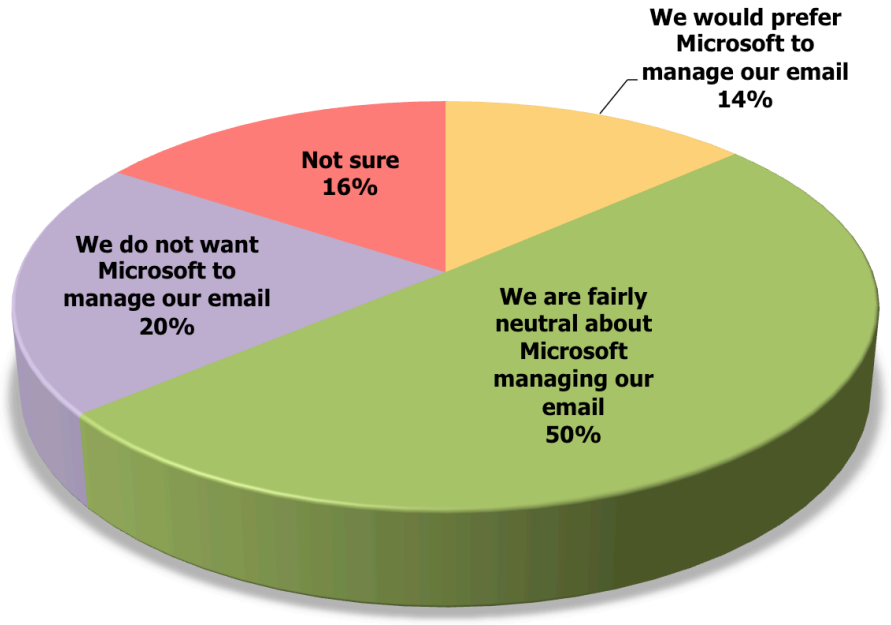
What services are offered for migrating existing, on-premise Exchange mailboxes and email security settings to Office 365?

- Are there exit strategies available on a number of levels: a) moving back from Office 365 to some sort of an on-premise email capability, or b) moving from cloud-based archiving to on-premise archiving while leaving email in the cloud.

SHOULD MICROSOFT MANAGE YOUR EMAIL?

- Another important consideration is whether or not Microsoft (or any single cloud vendor) should manage all of an organization's email. When we asked this question specifically about Microsoft, we found that many decision makers and influencers were not supportive of having Microsoft manage their corporate email, as shown in the following figure.

Views on Having Microsoft Manage an Organization's Email Infrastructure



SINGLE SIGN-ON ISSUES

- Is single sign-on required?
- If so, will the investment in on-premise Microsoft solutions be worth the expense, or will another single sign-on offering be a better fit?
- If a third party is used, will that party leverage Microsoft's ADFS for identity management and single sign-on as opposed to other, non-Microsoft-sanctioned/approved methods?

MOBILITY ISSUES

- Which mobile platforms are used today and which ones will be used in the future?
- How well will our mobile users be supported in Office 365 and by third party providers?

INTEGRATION AND SUPPORT ISSUES

- What types of support services are available with the providers we are considering? Online support only, telephone support, chat support, concierge onboarding, US-based support?

How well can a third party vendor integrate with Office 365 from a user management and Active Directory sync perspective?

- How much support will be required initially and long term?
- How well can a third party vendor integrate with Office 365 from a user management and Active Directory sync perspective?

PROFESSIONAL SERVICES ISSUES

- To what extent will Microsoft-focused professional services be required to assist in the migration and/or integration process?
- To what extent will deep product integration with Microsoft services and software be required?
- How much will providers be required to know about Microsoft's underlying technology, including key Microsoft-focused competencies and certifications? How much do they know?
- How much experience should the provider have with multiple Microsoft platforms like Office 365, BPOS, on-premise Exchange, Exchange Online, SharePoint, Lync, etc.?
- Does the provider have direct access to internal Microsoft product team internal resources, training materials and technical content?

OTHER ISSUES

- How well can a hybrid deployment of Office 365 and on-premise systems be managed?

SUMMARY

Office 365 is a solid offering from the world's leading software company. It provides a number of useful features across a wide range of price points and is designed to satisfy many of the messaging, application and content management needs of individual users through very large enterprises. Despite its many capabilities, as a generalist product offered to a mass market it is not capable of satisfying every requirement from every organization. Consequently, many organizations will need to employ supplementary security, archiving, encryption and other capabilities to fill in the feature, function and reliability gaps they will experience when using an Office 365-only deployment.

SPONSOR OF THIS WHITE PAPER

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe. http://www.mcafee.com.

For more information about McAfee Email Protection, McAfee SaaS Email Archiving, McAfee Web Protection, and McAfee Cloud Single Sign On, please visit: http://www.mcafee.com/emailwebsecurity.

www.mcafee.com

@McAfee

+1 888 847 8766

CITATIONS

[i] http://www.slashgear.com/analysts-question-microsoft-office-365-adoption-rate-23278972/

[ii] http://www.pcworld.com/article/2036178/microsoft-says-office-365-adoption-accelerating-but-questions-remain.html

[iii] According to Microsoft, "the new Exchange DLP features identify, monitor, and protect sensitive data through deep content analysis. Exchange offers built-in DLP policies based on regulatory standards such as PII, HIPAA, and PCI, and is extensible to support other policies..."

[iv] Office 365 Enterprise Plans support external journaling to a third party archive, but non-Enterprise plans do not support journaling.

[v] http://office.microsoft.com/en-us/business/office-365-security-and-privacy-verified-by-a-third-party-FX103089231.aspx

[vi] http://technet.microsoft.com/en-us/library/jj819299.aspx

[vii] http://technet.microsoft.com/en-us/library/jj819299.aspx

[viii] http://technet.microsoft.com/en-us/library/jj822177.aspx

[ix] http://technet.microsoft.com/en-us/library/jj822177.aspx

[x] http://office.microsoft.com/en-us/outlook-help/license-requirements-for-personal-archive-and-retention-policies-HA102576659.aspx

[xi] https://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p037553.pdf

[xii] http://help.outlook.com/140/dd630704.aspx

[xiii] http://help.outlook.com/140/dd630704.aspx

[xiv] http://community.office365.com/en-us/wikis/exchange/throttling-limits-for-office-365.aspx

[xv] http://help.outlook.com/140/dd630704.aspx

[xvi] http://help.outlook.com/140/dd630704.aspx

[xvii] http://www.o365info.com/2012/11/recover-deleted-mail-items-office-365.html#SUB-10

[xviii] http://office.microsoft.com/en-us/office365-sharepoint-online-enterprise-help/sharepoint-online-software-boundaries-and-limits-HA102694293.aspx#_SharePoint_Online_for_2

[xix] http://www.msdigest.net/2013/03/the-limits-of-shared-mailboxes-in-office-365/

[xx] http://technet.microsoft.com/en-us/library/dn144876(v=exchg.150).aspx

[xxi] http://www.storagecraft.com/blog/migrating-to-office-365-important-things-to-consider/

[xxii] http://www.storagecraft.com/blog/migrating-to-office-365-important-things-to-consider/

[xxiii] http://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Geo_Boundaries.htm

[xxiv] http://thoughtsofanidlemind.wordpress.com/2013/04/29/upgrading-office-365-wave-15/

[xxv] Source: *Office 365™ Security* white paper

[xxvi] http://technet.microsoft.com/en-us/library/jj723119(v=exchg.150).aspx

[xxvii] http://technet.microsoft.com/en-us/magazine/jj631606.aspx

[xxviii] Microsoft Exchange Online Dedicated Plans Versions Service Level Agreement (SLA), October 2012

[xxix] http://help.outlook.com/en-US/140/ms.exch.ecp.learnmoreretentiontags.aspx

[xxx] http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225

[xxxi] http://www.washingtontimes.com/news/2013/may/17/irs-sued-seizing-60-million-medical-records/

[xxxii] http://blogs.msdn.com/b/microsoft_press/archive/2013/04/29/from-the-mvps-data-loss-prevention-with-office-365-and-exchange-online.aspx

[xxxiii] http://technet.microsoft.com/en-us/library/jj150512(v=exchg.150).aspx

[xxxiv] http://technet.microsoft.com/en-us/library/jj150541(v=exchg.150).aspx

[xxxv] http://help.outlook.com/en-us/140/ee424425.aspx

[xxxvi] http://community.office365.com/en-us/forums/158/t/84239.aspx

[xxxvii] http://office.microsoft.com/en-us/sharepoint-help/create-and-run-ediscovery-queries-HA102922715.aspx?CTT=3

[xxxviii] http://technet.microsoft.com/en-us/library/jj891031.aspx