WHITE PAPER

Microsoft® Office 365® for the Enterprise: How to Strengthen Security, Compliance and Control

An Osterman Research White Paper

Published February 2015

intel® Security

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 robust set of email and collaboration tools that is offered in a number of configurations with varying levels of features and functions. Office 365 represents Microsoft's latest – and arguably, most successful – venture into the cloud services space in the 13+ years that the company has offered hosted services.

KEY TAKEAWAY

Despite the range of functionality offered in Office 365, like any cloud-based offering it cannot be all things to all customers. There are some missing features in Office 365 that will prompt some customers to consider the use of third-party, cloud-based or on-premises tools to enhance Office 365's native capabilities. Specifically, we believe that these third party enhancements will be focused primarily on the security, archiving and encryption capabilities available with Office 365. That is not to say that Microsoft has not addressed these capabilities, but many third parties provide more granular or more capable services than Microsoft has offered in Office 365. Osterman Research believes that the third-party market for cloud-based and on-premises capabilities designed to supplement or replace specific Office 365 features and functions will grow at a healthy pace along with the market for Office 365.

AN IMPORTANT NOTE

The purpose of this white paper is not to dismiss Office 365, its features and functions, or Microsoft itself. On the contrary, we believe that Office 365 provides a useful set of features and functions that will be well received by many organizations. However, our goal is to be as fair and balanced as possible in discussing both the advantages and disadvantages of Office 365. As with any cloud-based service, there are limitations in Office 365 that can be managed more appropriately through the use of third party services. Any limitations discussed here are not limited to Office 365, but can be said for any cloud-based solution.

ABOUT THIS WHITE PAPER

This white paper discusses the Office 365 environment, its applicability for organizations of all sizes, and the third party capabilities that Office 365 customers should consider to supplement the platform. This document also provides a brief overview of its sponsor – McAfee – and the company's relevant offerings.

KEY FEATURES AND FUNCTIONS OF OFFICE 365

Office 365 represents Microsoft's newest foray (in quite a long line of them) into the cloud-based email and collaboration space. The platform is a group of cloud-based offerings that includes Exchange Online (most accounts offer 50-gigabyte mailboxes), SharePoint Online, Lync Online, and desktop and Web-based versions of Microsoft's productivity applications. The various components and offerings in Office 365 are shown in Figure 1.

Office 365 represents Microsoft's newest foray (in quite a long line of them) into the cloud-based email and collaboration space.

Figure 1
Versions and Costs for Office 365 (US pricing)

Version	Includes	$/User/ Month
Office 365 Small Business	Email, online conferencing, public Web site, file share, Office Web apps	$5.00
Office 365 Small Business Premium	Same as above plus desktop versions of all Office applications	$12.50
Office 365 Midsize Business	Same as above plus Active Directory integration	$15.00
Exchange Online Plan 1	Email, Active Directory integration	$4.00

Figure 1 (concluded)
Versions and Costs for Office 365 (US pricing)

Version	Includes	$/User/ Month
Office 365 Enterprise E1	Same as above plus file sharing, online conferencing, enterprise social, Office Web apps	$8.00
Office 365 Enterprise E3	Same as above plus desktop versions of all Office applications, eDiscovery Center	$20.00
Office 365 Enterprise E4	Same as above plus Yammer Enterprise, other features	$22.00

Source: Microsoft

Organizations are migrating to Office 365 because of its advantages, which generally apply to cloud-based email and collaboration systems:

- Lower and more predictable costs of ownership
- Faster deployment of new services
- The ability to upgrade or downgrade capabilities quickly and easily
- The ability to free IT staff for other tasks
- The ability to add new capabilities that would require either the addition of new staff members or access to expertise that is not readily available internally

GROWING USE OF OFFICE 365

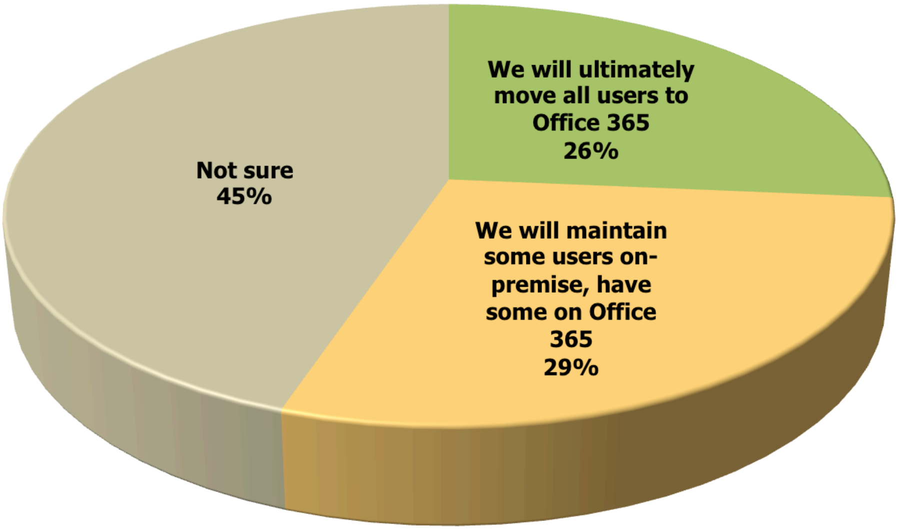
Office 365 growth has been quite robust:

- Microsoft reached one million Office 365 Home Premium subscribers in May 2013[i], two million by October 2013[ii] and 3.5 million by early 2014[iii].
- Microsoft claims that more than one million US government employees use Office 365[iv].
- Microsoft estimates that more than 15% of its Exchange installed base is now using Office 365[v].
- In 2014/Q2, Microsoft reported that it more than doubled its commercial cloud services revenue[vi].

As shown in Figure 2, the Osterman Research survey conducted for this white paper found that most organizations plan to migrate some or all of their users to Office 365 in the near- to mid-term.

Most organizations plan to migrate some or all of their users to Office 365 in the near- to mid-term.

Figure 2
Organization's Plans for Migrating to Office 365
Among organizations that are considering a migration to Office 365



Source: Osterman Research, Inc.

Microsoft has made Office 365 compliant with a number of important standards and other requirements as verified by various third parties.

OFFICE 365 CAN BE USED IN REGULATED ENVIRONMENTS

Although Microsoft has been providing cloud-based email for a number of years, the current versions of their cloud offerings are quite robust and offer a number of enterprise-grade features and functions. In addition, Microsoft has made Office 365 compliant with a number of important standards and other requirements as verified by various third parties[vii], further enhancing its potential for use by enterprise customers:

- The Federal Information Security Management Act (FISMA)
- Business Associate Agreements under the Health Insurance Portability and Accountability Act (HIPAA)
- 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)
- International Organization for Standardization (ISO) 27001
- European Union (EU) Safe Harbor and Data Protection Directive Model Clauses

The result is that Office 365 may be used in regulated environments, such as healthcare, government and also in the European Union. Microsoft also benefits from support for a hybrid model given that it has a commanding market share for desktop productivity applications and its dominance in the business email market through Exchange. This gives Microsoft an advantage that many competitors cannot enjoy.

WHAT ARE THE DRAWBACKS OF OFFICE 365?

Although there are a number of advantages associated with using Office 365, there are some limitations about which decision makers should be aware:

ARCHIVING LIMITATIONS

- Migration to Office 365 has been problematic for some organizations, particularly those that want to maintain a hybrid deployment of on-premises and cloud-based users.

- Microsoft's 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. In addition, some Outlook versions are not supported[viii].

- The archiving functionality in Office 365 has some additional limitations, including lack of support for Exchange Online archiving with Outlook 2011 under Mac OS X[ix], as well as lack of support for accessing archived emails via Android and iPhone devices.

- According to Microsoft, "You can't designate an Office 365 mailbox as a journaling mailbox for on-premises mailboxes. If you're running a hybrid deployment with your mailboxes split between on-premises servers and Office 365, you can designate an on-premises mailbox as the journaling mailbox for your Office 365 and on-premises mailboxes."[x]

- Some versions of Office 365 do not archive instant messaging content, conference content, or content from application-sharing or desktop-sharing sessions[xi]. Some versions of standalone Lync Online plans do not provide instant message and file filtering, instant message content archiving, or conference content archiving[xii].

- SharePoint Online offers eDiscovery, compliance with various regulatory obligations and other capabilities, but it does not archive content. Because of the growing proportion of content that is stored in SharePoint within the organizations that have deployed it, the ability to archive SharePoint content is essential.

- End user search capabilities in some versions of Office 365 are somewhat more limited than they are with many competing cloud-based and on-premises archiving solutions.

- Office 365 includes no native surveillance features that allow monitoring or sampling of communications. This is an important capability for highly regulated firms, such as broker-dealers that must sample communications per FINRA Regulatory Notice 07-59[xiii].

- For organizations that need to journal content into Office 365 – such as Salesforce Chatter content, instant media, social posts, etc. – a third party archiving solution will be required, since journaling within Office 365 does not support import of external, non-Lync content.

Migration to Office 365 has been problematic for some organizations, particularly those that want to maintain a hybrid deployment.

RETENTION LIMITATIONS

- Only Office 365 Plans E3 and E4 include the ability to search across Exchange mailboxes and SharePoint sites, Information Rights Management, archiving, litigation hold capabilities and unlimited storage[xiv].

- The maximum size of the arbitration mailbox is ten gigabytes[xv].

- Items in the Office 365 Deleted Items and Junk E-Mail folders can be retained for a maximum of 30 days[xvi].

DATA LOCATION LIMITATIONS

- Microsoft stores Office 365 customer data in a number of different countries based on the location of the customer[xvii]. Moreover, Microsoft can move customer data without notice and will not guarantee exactly where a customer's data will be stored. For example:

  - Government customers in the United States: primary data and backup centers are located in the United States.

  - North American customers: primary data 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 notes that it will not provide notice when customer data is transferred to a new country and that "the requirements of providing the services may mean that some data is moved to or accessed by Microsoft personnel or subcontractors outside the primary storage region." Office 365 and Microsoft Dynamics CRM Online data centers are located worldwide and store data based on the location of its customers:

  - North American and South American customers: US data centers
  - Brazilian customers: US and Brazilian data centers
  - European Union customers: US, Irish and Dutch data centers
  - Asia-Pacific customers: US, Singapore and Hong Kong data centers

Office 365 does not directly support the deployment of redundant spam filters in parallel with Office 365's built-in spam protection.

SECURITY LIMITATIONS

- All Office 365 plans offer administrator management of the spam quarantine, but some plans allow this only via direct access to the Exchange Admin Center management interface[xviii].

- Office 365 does not directly support the deployment of redundant spam filters in parallel with Office 365's built-in spam protection.

- Instant messaging and file filtering are not available with any Office 365 plans[xix].

- Office 365 does not offer more advanced and targeted threat protection techniques, such as real-time link following that emulates the contents for malware, in addition to reputation checks.
- Office 365 does not support taking an action on an email containing a link strictly based off the URL reputation alone.

- Office 365 does not help users on mobile devices determine whether a link in an email is safe to click on.

MOBILITY LIMITATIONS

- BlackBerry Enterprise Server (BES) is not supported by Microsoft in Office 365, although BlackBerry Business Cloud Services supports Office 365[xx]. Despite declining support for BES in some organizations, this is a serious problem for organizations that still have many BlackBerry users (and there are still many of them out there).

- Office 365 will wipe only those mobile devices that are managed using ActiveSync.

- 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 LIMITATIONS

- 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. The contents of a deleted mailbox can be recovered for 30 days after deletion, but both the mailbox and its contents will not be recoverable after 30 days if the hold is not activated[xxi].

- Microsoft provides shared mailboxes in Office 365 at no charge, but they cannot be larger than 10 gigabytes and can be created only with Remote PowerShell. Add to this the fact that a shared mailbox cannot be accessed by users of an Exchange Online Kiosk license and cannot archive emails from individual users[xxii].

Office 365 does not provide specific control over when users will be upgraded – only Microsoft determines when upgrades occur.

OS AND APPPLICATION VERSION LIMITATIONS

- The minimum supported versions of Outlook clients that can be used are Outlook 2013, 2010 and 2007 (with some limitations in functionality) for Windows; and Outlook 2011 for Mac[xxiii]. Interestingly, Microsoft indicates that Office 365 also supports Outlook 2008 for Mac, although Office 2008 for Mac included only Entourage.

- Office 365 support for Windows XP/SP3 and Vista SP2 ended on December 31, 2013[xxiv].

OTHER LIMITATIONS

- Office 365 does not provide specific control over when users will be upgraded – only Microsoft determines when upgrades occur[xxv].

- While single sign-on is supported in Office 365, it is supported only with Active Directory Federation Services 2.0[xxvi].

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

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

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

IMPROVING SECURITY IN OFFICE 365

Microsoft provides 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 limitations that decision makers should take into account as they consider a migration to Office 365. These include:

- **The use of a multi-tenant architecture**
  Office 365 employs a multi-tenant architecture, dictating that multiple customers' environments run on the same servers. While this *can* provide a secure management environment, there are organizations – particularly those in heavily regulated industries or those that manage confidential or sensitive information – that may not find the use of such a shared data environment feasible. Although Microsoft isolates customer data into silos, the company offers the ability to store Office 365 data on dedicated hardware for an additional cost[xxvii].

- **Additional security layers may be needed**
  Microsoft Exchange Online Protection (EOP)[xxviii] uses several scanning engines from leading security vendors. EOP's Service Level Agreement (SLA) claims to detect 100% of all *known* viruses with updates every 15 minutes.

  However, some customers may want to add an additional layer of inbound protection in order to improve abilities for phishing or spearphishing detection capability, as just one example. Alternatively, they may simply want to add another layer of malware or spam filtering for additional protection beyond what Microsoft provides.

  Graymail capabilities have been added to EOP, but it 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' needs. In addition, Lync Online does not scan files or other content for malware. 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 cannot open phishing messages and have their PC and the corporate network potentially compromised).

- **Advanced threat protection**
  Office 365 may not provide the complete level of protection from advanced threats that many organizations will need. 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 in order to block those that are malicious, or block those whose intent has been changed to malicious from the time the message was sent. Because many larger organizations will need to wrap advanced security capabilities like these around Office 365, the basic security capabilities in Office 365 will need to be evaluated in light of decision makers' attitudes toward risk.

- **Mobility limitations**
  Office 365 will wipe only ActiveSync devices. This can be a serious limitation for the large number of organizations that still support BlackBerry devices and do not want to do so via ActiveSync. Plus, while all versions of Office 365 support the BlackBerry Internet Service, not all versions support BlackBerry Business Cloud Services. Although BlackBerry supports ActiveSync, there have been some reported problems. 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, but this will add to the cost of Office 365.

Microsoft manages all of the backup and recovery of content for Office 365 customers unless they have implemented their own capabilities at an additional cost.

- **Microsoft is responsible for Office 365 backup and recovery**
  Microsoft manages all of the backup and recovery of content for Office 365 customers unless they have implemented their own capabilities at an additional cost. Moreover, there are no native selective restore capabilities. While Microsoft's management of backup and recovery is not necessarily an inherent weakness, customers must rely on Microsoft to manage this part of the Office 365 experience and to do so in a timely manner.

- In summary, Office 365's included security is quite reasonable, but it does not offer all of the advanced protection features of a dedicated security provider. Consequently, security in Office 365 may not be the most suitable security solution for every organization.

THE OFFICE 365 SLA MAY NOT BE ADEQUATE FOR EVERYONE

Microsoft offers a reasonable SLA for Office 365[xxix]. However, it is important for decision makers to evaluate whether or not this SLA will meet their requirements. For example, key provisions of the Office 365 SLA include:

- "Service Credits are your sole and exclusive remedy for any performance or availability issues for any Service under the Agreement and this SLA."

- 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] control", "that result from your or third party services, hardware, or software", or "during pre-release, beta and trial Services (as determined by us)".

Microsoft determines "monthly uptime" in a way that fairly high levels of downtime could be experienced by some Office 365 users, but not trigger the payment of Service Credits. For example, consider a 1,000-user organization with 800 users in North America and 200 users in Europe. If the European customers dealt with 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%. The result is that although the European users experienced uptime of only 99.51% during the month, no Service Credits would be paid.

IMPROVING COMPLIANCE CAPABILITIES IN OFFICE 365

Many decision makers do not consider all of their long-term archiving and compliance requirements before migrating to a cloud-based messaging platform. For example, an organization may not plan for the archival of social media, text messaging or other content types that they do not archive today, but might need to in the future as a result of regulators' or courts' decisions. However, when migrating email and collaboration to the cloud, a new set of compliance considerations becomes important to understand before any decisions are made.

Many decision makers do not consider all of their long-term archiving and compliance requirements before migrating to a cloud-based messaging platform.

A FOCUS ON KEY ARCHIVING CAPABILITIES

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

For example, only Office 365 Plans Enterprise E3 and E4 offer unlimited archive storage quotas and litigation hold capabilities, which means that users not provisioned with these more expensive Office 365 plans may require supplemental archiving capabilities to ensure adequate retention of their data. Further, the other plans share storage between the primary mailbox and the archive, whereas the E3 and E4 plans do not. If supplemental archiving capabilities are required, this will negate 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. 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."*[xxx]

The result is that some organizations with strict requirements for retaining all relevant messages, such as broker-dealers, may need to seek alternative archiving solutions that will ensure retention of all relevant messaging content.

GEOGRAPHIC AND JURISDICTIONAL REQUIREMENTS

Many organizations must satisfy a variety of obligations to comply with different jurisdictional requirements, such as a requirement that data not leave a particular geographic area or that it is not moved to a nation that does not offer adequate protection of sensitive data. Microsoft stated in July 2013 that it provides "customer data [to law enforcement] only in response to legal processes[xxxi]", although the company is certainly alone in doing so. Also, since customer data can be moved to a variety of locations for day-to-day management or backup purposes, this can create jurisdictional problems for companies that have strict rules about data location.

Some third-party archiving solutions offer more control and transparency about where customer data resides, which may alleviate decision makers' concerns. This is particularly true for non-US customers that may not want their data accessed – especially accessed without their knowledge – under the PATRIOT Act, by the IRS[xxxii] or by other US government agencies.

Another important consideration that applies to all cloud providers is the issue of blind subpoenas – subpoenas issued by a government authority without the knowledge of the customer. Because a provider can be compelled to give 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. Cloud providers that can guarantee storage of customer data in a non-US location may be considered preferable for that small segment of the market that wants this capability.

One limitation of Office 365 is that during downtime periods, the archived content is unavailable.

THE ADVANTAGE OF A SEPARATE ARCHIVING PROVIDER

One limitation of Office 365 is that during downtime periods, the archived content is unavailable. The use of a third party archiving solution independent from Microsoft's will eliminate this problem by storing data in a separate infrastructure, allowing users to access their archived content even while their primary email functionality is down. This is a key component of a business continuity solution, allowing users 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, during one month in 2013, there were four major outages that affected Microsoft's online services.

DATA LOSS PREVENTION

Microsoft has implemented data loss prevention (DLP) in Office 365, Exchange Online and Exchange 2013 based on Exchange Transport Rules[xxxiii]. By using Policy Tip notification messages, Outlook users can be alerted to possible violations of corporate policies when sending email that could contain sensitive or confidential information[xxxiv]. Microsoft has provided a number of definitions[xxxv] that can be used in its standard offering, but allows administrators to develop and publish custom definitions, as well.

As of today, DLP Policy Tips used with Exchange Online can be used with Outlook 2013, OWA or OWA for Devices[xxxvi]. These DLP policies work for emails sent from other clients, but the Policy Tips feature works only with these platforms. Advanced capabilities like file fingerprinting are not available.

eDISCOVERY AND LITIGATION HOLD CAPABILITIES

The Enterprise E3 and E4 plans provide built-in eDiscovery capabilities through the eDiscovery Center, but some organizations will need more sophisticated and granular functionality. These might include highly configurable legal holds and robust case management when performing online reviews, for example. Some organizations that have sophisticated requirements will find that although useful, Office 365's built-in eDiscovery capabilities might not meet their needs.

There are some eDiscovery limitations in Office 365, such as:

- Reviewing data that results from a search can be more difficult in Office 365 than with some third party tools. Because search results are copied to a discovery mailbox and subsequently accessed via Outlook or OWA, this can make the review of a large number of search results or sharing the responsibility of reviewing content across groups more time consuming. Insufficiently sophisticated review tools is an important issue for organizations that need to perform early case assessments or other types of operations across the entire organization[xxxvii].

- 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 must be captured for more than this number of mailboxes, the process must be repeated and content stored in batches of 50 mailboxes. An alternative is for IT to use the Exchange Management Shell command-line interface to manage discovery[xxxviii].

- When the eDiscovery Center in SharePoint Online is used, a search query across a maximum of 1,500 Exchange sources and 100 SharePoint is possible. If more mailboxes must be searched, then multiple search queries must be run or the Exchange Management Shell command-line interface must be used[xxxix].

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

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

Some 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.

- Better support for EDRM requirements..

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

SOME PLATFORMS AND CONTENT SOURCES ARE NOT SUPPORTED

Some organizations maintain several on-premises and cloud-based messaging, collaboration or storage platforms, and so will require an archiving and compliance solution that will support all of them. Microsoft's archiving solutions do not currently support all of the platforms that an organization might have in place, such as GroupWise, Notes/Domino, Google Apps, Box or Dropbox, among many others. 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 their SharePoint content.

For many organizations, this will be an important consideration. Because an eDiscovery effort, for example, can be made more complicated and more expensive if an organization must extract content from multiple archiving systems – such as one for Office 365, one for SharePoint content or one for files stored in the cloud – having one, corporate-wide archiving solution for all content will speed eDiscovery, litigation holds and other activities, as well as drive down their cost.

LIMITATIONS IMPACTING STORAGE

Many organizations store 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.

ADDITIONAL ISSUES TO CONSIDER

Decision makers will also need to answer four basic questions when deciding 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 existing email archive to Office 365?

2. Should we migrate our active mailboxes 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:

ARCHIVING AND CONTENT MANAGEMENT CONSIDERATIONS

- Do we need redundant copies of our archived data in multiple, geographically separate 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 or will not be stored?

- 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?

For some customers, the limitations in Office 365's archiving for the less expensive plans will not be acceptable.

- What will be the impact of the US PATRIOT Act and other governmental actions on our ability to protect information?

- What options are available for maintaining an on-premise archive of cloud-based content?

BUSINESS CONSIDERATIONS

- Should we employ multiple providers in order to distribute the risk associated with going to the cloud? 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 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.

- 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?

- 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?

- 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?

- 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?

REGULATORY CONSIDERATIONS

- 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?

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

SERVICE LEVEL CONSIDERATIONS

- What should our backup strategy for Office 365 data be?

- 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 metrics do we need to establish with regard to Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)?

- What compensation is offered by providers following outages?

Is Office 365 able to meet our requirements for uptime/ availability?

MIGRATION CONSIDERATIONS

- Are there exit strategies available for a) migrating 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?

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

- What services are offered for migrating from on-premises SharePoint to Office 365?

- Do these services include mail route control, split domains or blended solutions that can streamline the migration process?

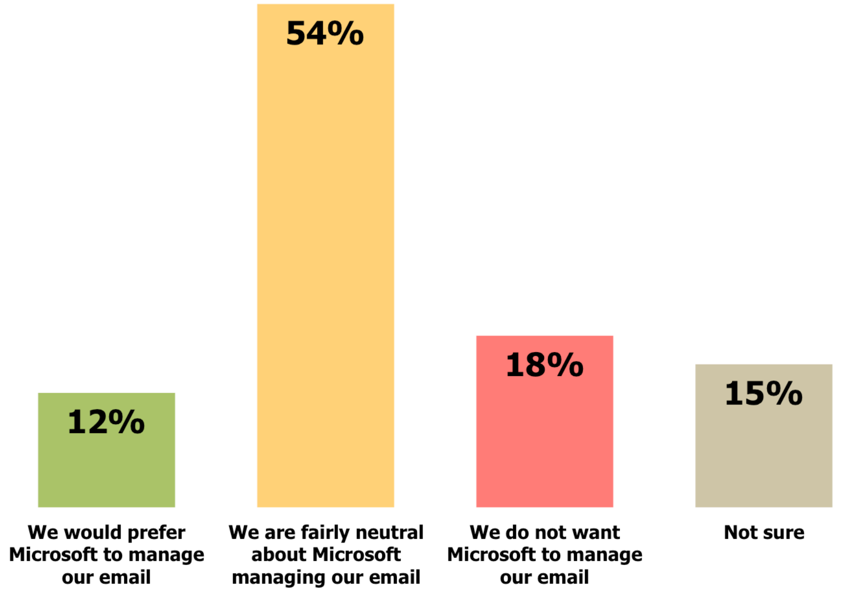
- To what extent are customization services necessary?

DO WE WANT MICROSOFT TO MANAGE OUR EMAIL?

- Should Microsoft manage our email services? When we asked this question specifically about Microsoft, we found that many decision makers and influencers are not supportive of having Microsoft manage their corporate email, as shown in Figure 3.

Many decision makers and influencers are not supportive of having Microsoft manage their corporate email.

Figure 3
Opinions on Having Microsoft Manage the Email Infrastructure



Source: Osterman Research, Inc.

MOBILITY CONSIDERATIONS

- Which mobile platforms are used today and which ones will be used in the future?
- Will Microsoft provide the needed support for Android-based and iOS-based mobile platforms in the future?
- How well will our mobile users be supported in Office 365 and by third party providers?
- How well are users protected from malware when reading emails on their mobile devices, such as links to malware that are contained in emails?

INTEGRATION AND SUPPORT CONSIDERATIONS

- How much support will be required initially and long term?
- What 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?

PROFESSIONAL SERVICES CONSIDERATIONS

- To what extent will deep product integration with Microsoft services and software be required?
- To what extent will Microsoft-focused professional services be required to assist in the migration and/or integration process?
- How much experience should a third party provider have with multiple Microsoft platforms like Office 365, on-premise Exchange, Exchange Online, SharePoint, Lync, etc.?
- 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?
- Will the provider(s) have direct access to internal Microsoft product team internal resources, training materials and technical content?

SUMMARY

There is no denying that Microsoft Office 365 is a robust offering that offers a wide range of capabilities. Microsoft has taken pains to ensure that Office 365 operates with reasonable reliability and that its features and functions meet the needs of a wide range of potential customers. However, as with any mass-market, technology-based offering there will be deficiencies in specific aspects of the features and functions that many customers require. Because no cloud-based offering can be all things to all customers, many – if not most – Office 365 customers will require third party products and services to supplement the native capabilities of the platform.

Because no cloud-based offering can be all things to all customers, many – if not most – Office 365 customers will require third party products and services to supplement the native capabilities of the platform.

SPONSOR OF THIS WHITE PAPER

McAfee is now part of Intel Security. With its Security Connected strategy, innovative hardware-enhanced security, and unique Global Threat Intelligence, Intel Security develops proactive, proven security solutions and services to protect systems, networks, and mobile devices for business and personal use all over the world. www.intelsecurity.com.

McAFEE THREAT PROTECTION FOR OFFICE 365

McAfee Email Protection for Microsoft Office 365 Exchange Online helps stop targeted phishing attacks and provides customizable warning pages to reinforce user training. Faster threat detection and reliable email continuity provides assurance, while deployment flexibility enables enterprise-grade security to move with your mailboxes, anywhere they reside.

- The combination of McAfee Global Threat Intelligence which collects real-time data from over 100 million sensors across file, web, email, and network vectors, multiple antivirus engines, and over 20 separate filters eliminate over 99% of spam and viruses before they hit hosted Exchange.

- Click-Time scanning of links within email detects changes in URL intent between when a message is scanned and when a link is clicked, even on mobile devices. Links are subjected to real-time emulation and behavioral analysis of URL content – a technique which has proven to stop over 95% of zero-day malware and prevent targeted attacks.

- Graymail messages are clearly identified in end-user spam reports, allowing for simple identification amongst standard spam. End-user management is available to allow self-selection of graymail handling, such as denying, tagging, or allowing these messages.

- For the most advanced email threats, McAfee Advanced Threat Defense integrated with McAfee Email Protection can detect stealthy or delayed malware using static and dynamic analysis. Suspicious files found in email are sent to McAfee Advanced Threat Defense and observed in a sandbox environment while simultaneously disassembled for thorough analysis.

- Email Continuity enables full access to a web interface where users can access email during any planned or unplanned outages of their hosted email service.

McAFEE DATA PROTECTION FOR OFFICE 365

- When layered over Office 365, outbound email can be analyzed and acted upon with further granularity than provided in any offering by Microsoft, providing the level of data protection needed for businesses with sensitive or regulated data. Over 100 prebuilt compliance templates allow administrators to take action upon emails which violate HIPAA, PCI-DSS, SOX, and other regulations, including the ability to encrypt messages or block them from leaving the organization.

More information can be found at mcafee.com/emailsecurity.

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, statue, 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.

REFERENCES

[i] http://www.zdnet.com/microsoft-1-million-office-365-home-premium-subscribers-on-board-7000016052/

[ii] http://www.zdnet.com/microsoft-hits-2-million-plus-office-365-home-premium-subscriber-mark-7000022421/

[iii] http://www.zdnet.com/office-365-after-one-year-hows-microsoft-doing-7000026585/

[iv] http://www.microsoft.com/en-us/news/cloud/index.html

[v] http://www.zdnet.com/office-365-after-one-year-hows-microsoft-doing-7000026585/

[vi] http://www.microsoft.com/investor/EarningsAndFinancials/Earnings/PressReleaseAndWebcast/FY14/Q2/default.aspx

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

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

[ix] http://support.microsoft.com/kb/2830042

[x] http://technet.microsoft.com/en-us/library/aa998649(v=exchg.150).aspx

[xi] http://technet.microsoft.com/en-us/library/lync-online-security-and-archiving.aspx

[xii] http://technet.microsoft.com/en-us/library/lync-online-security-and-archiving.aspx

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

[xiv] http://office.microsoft.com/en-us/business/compare-all-office-365-for-business-plans-FX104051403.aspx

[xv] http://technet.microsoft.com/library/exchange-online-limits(EXCHG.150).aspx

[xvi] http://technet.microsoft.com/library/exchange-online-limits(EXCHG.150).aspx

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

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

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

[xx] http://us.blackberry.com/business/software/cloudservices.html

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

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

[xxiii] http://office.microsoft.com/en-us/business/compare-all-office-365-for-business-plans-FX104051403.aspx

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

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

[xxvi] http://technet.microsoft.com/en-us/library/hh852486.aspx

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

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

[xxix] Service Level Agreement for Microsoft Online Services, January 1, 2014

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

[xxxi] http://www.microsoft.com/en-us/news/press/2013/jul13/07-11statement.aspx

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

[xxxiii] http://blogs.office.com/2013/10/28/office-365-compliance-controls-data-loss-prevention/

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

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

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

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

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

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