WHITE PAPER

Best Practices for Migrating to Office 365

An Osterman Research White Paper

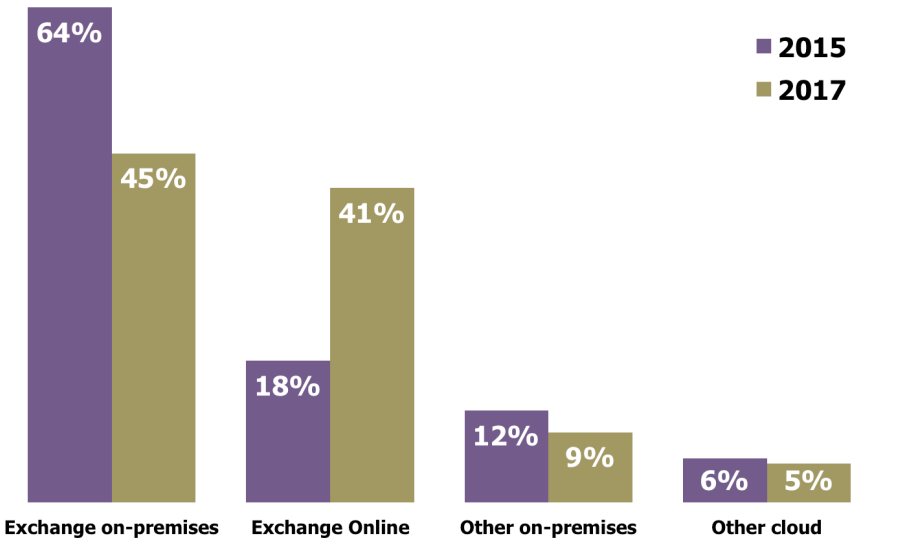
Published April 2015

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

Many organizations are seriously considering the deployment of Microsoft Office 365 and Exchange Online. The result is that the penetration of Office 365 is expected to more than double by 2017, primarily at the expense of on-premises Exchange, as shown in Figure 1.

Figure 1
Plans for On-Premises and Cloud-Based Email, 2015-2017



Source: Osterman Research, Inc.

MIGRATING TO OFFICE 365 IS A SIGNIFICANT UNDERTAKING

Migrating to Office 365 represents a significant step for an organization. It introduces product upgrades and brand new tools, opens the way for new work practices, and provides opportunities for re-imagining productivity. It also introduces a set of new demands and risks for the organization. For example:

- **New Versions and Devices**
  Most of the Office 365 plans provide access to new versions of current tools, whether that is the online editions of Word, Excel, PowerPoint, and OneNote; or the right to run Office apps on computers, mobile devices, and smartphones. The new versions have upgraded and new capabilities that users need to learn, and for touch-enabled devices, new user interaction paradigms.

- **New Tools**
  The more advanced plans in Office 365 offer new online tools to support collaboration and communication. For example, Delve uses machine-learning technologies to surface relevant content personalized to each user, keeping them informed about what is happening in their organizational network. Yammer provides a set of social tools for communication, sharing updates, and working together.

- **New Work Practices**
  The new tools in Office 365 allow for the introduction of new work practices, such as changing from using email for distributing in-progress documents to using OneDrive for Business, SharePoint, or Yammer. Employees can stop using their phone and embrace Lync Online for presence awareness, quick chats,

voice calls, and even video meetings. Multiple people can open the same document simultaneously, participating in a true document collaboration experience.

- **New and Different Server Capabilities**
  Organizations that have held onto older versions of server software on-premises, such as Exchange 2003, are suddenly faced with what to do with a decade of innovation as they gain access to the newer Online versions in Office 365. For all of the on-premises servers that can be replaced with Office 365 equivalents, there are new features, additional capabilities, and some significant differences in the Office 365 versions.

- **New Value-Added Services**
  Microsoft offers a number of value-added services for Office 365, such email security and email archiving for Exchange Online. Organizations will need to investigate whether the new value-added services from Microsoft will meet their compliance, email security, archiving, and eDiscovery requirements, or if a third-party service is a better fit for their needs.

- **New Places for Sharing Files**
  Organizations that have relied on file shares for storing and sharing documents face a plethora of new places for files to be stored, shared, classified, and managed in Office 365. Some file share content will be best directed to document libraries in SharePoint Online. Other content should go to an individual's OneDrive for Business. Still other content will need to be moved into Yammer. Add to this the need to respect access privileges for confidential and sensitive documents, and decision makers are faced with a significant migration and rethinking exercise to work through.

- **New Demands on Connectivity**
  Organizations leveraging cloud-based business applications require a distributed network architecture to optimize performance. The move to a distributed model gives individual site locations local Internet connectivity to ensure a robust and productive work environment is maintained. Traditional backhauling architectures are no longer suitable.

- **Loss of Control**
  Office 365 removes much of the administrative burden of managing an on-premises infrastructure for productivity, communication, and collaboration. However, that also means giving Microsoft control over the timing and rhythm for releasing upgrades to employees, which has significant impacts for both training and enablement.

- **Risks in Migrating from Exchange On-Premises to Exchange Online**
  Moving data from legacy on-premises servers to the new services in Office 365 is not risk free. On-premises Exchange Servers can be misconfigured and contain corrupted mailboxes and messages, which are issues that will need to be resolved prior to the migration. And actually just getting all of the current data from legacy servers to Office 365 in the correct way is a massive undertaking, which will impact current business operations for months if not years.

- **A Long Migration Process**
  Migration to Office 365 takes a significant amount of time, and is measured in months and years, definitely not days or weeks. Organizations must be prepared for the migration process to take much longer than expected and set aside sufficient budget to cover both the process itself and the issues that will invariably arise during the migration. The length of a migration is generally tied to the complexity of the current on-premises architecture, as well as the desired end state for the migration to Office 365.

In short, migrating to Office 365 presents a significant set of challenges, opportunities, and risks for the organization generally and the IT group specifically, and it needs careful and appropriate planning.

ABOUT THIS WHITE PAPER

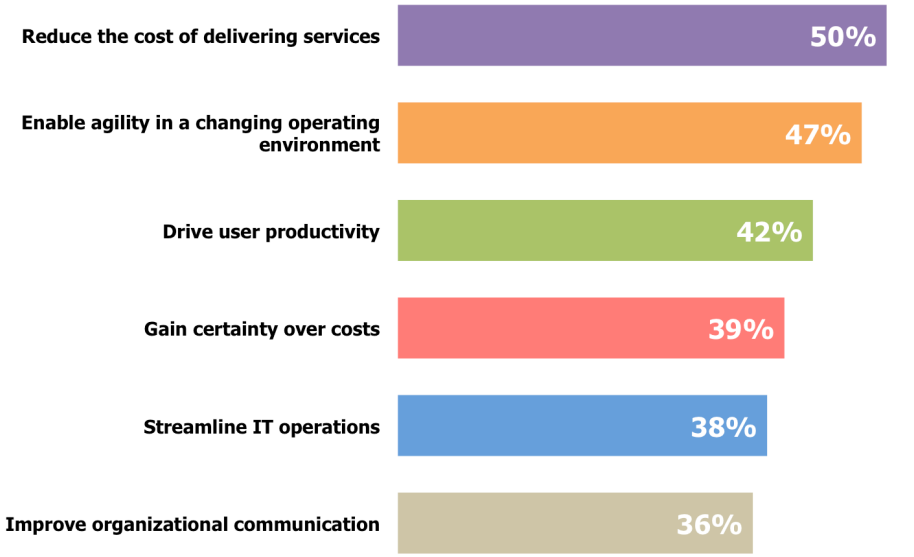
This white paper is intended to help decision makers understand the implications of migrating to Office 365, and it offers practical advice for doing so. The paper also provides data from a survey of current and prospective Office 365-enabled organizations that was conducted specifically for this white paper during March 2015.

The white paper was sponsored by Trend Micro – information on the company is provided at the end of the paper.

BUSINESS DRIVERS FOR MIGRATING TO OFFICE 365

While cost reduction is frequently cited as the main reason for moving to Office 365 – and with good reason – additional business drivers should feature prominently in the business case. The key business drivers for migrating to Office 365 uncovered in the survey we conducted for this white paper are shown in Figure 2.

Figure 2
Drivers for Deploying Office 365
% Responding Important or Extremely Important



Source: Osterman Research, Inc.

Expected short term cost reductions can quickly evaporate through a challenging and costly migration, or disappear entirely through poor planning for consequential cost increases, such as improved Internet connectivity. The business value of Office 365 is much greater than a few calculations in a spreadsheet can portray. Business drivers beyond cost reduction include:

ENABLE BUSINESS AGILITY

Dealing with mergers and acquisitions, opening new offices, and moving into new territories has often required the expansion of current on-premises infrastructure to support new locations and new employees. At times the construction of another data center has even been required. With Office 365, however, comes the ability to quickly scale up (and down) the number of licenses required for core productivity, communication, and collaboration tools as business needs dictate. IT again becomes an enabler of agility, not a roadblock to executing on decisions.

DRIVE USER PRODUCTIVITY

Users gain access to familiar Office productivity tools on a range of mobile devices and smartphones, setting the stage for productivity and contribution from wherever they are. This more flexible working environment means work can be done at the point of need – whether in a meeting with a client or during a coffee catch-up with a colleague – without having to wait for the employee to get back to the office. Work becomes an activity employees perform, not a place they to which they go.

GAIN CERTAINTY OVER COSTS

Office 365 plans are available at a fixed subscription rate, giving certainty over costs for planning and budgeting purposes. Upgrades and the introduction of new features and capabilities are seamlessly managed by Microsoft, eliminating the need for expensive migration projects that have become standard practice in the Microsoft ecosystem.

Moreover, it is important to understand that accurate cost savings from the deployment of Office 365 can be calculated, but typically only for organizations that understand the current cost of their on-premises IT infrastructure. General industry cost models are available to derive an estimate of current and future costs for organizations lacking in this area, but it is always best to have a specific and tested cost model against which to compare the future state with Office 365.

STREAMLINE IT OPERATIONS

Managing an on-premises infrastructure is a challenging proposition, with many layers of technical requirements, cross-product dependencies, and potential points of failure. Upgrading a single element in an organization's infrastructure may kick off a wave of linked upgrades, or cause a cascading set of errors as incompatibilities between servers erupt. Migrating to Office 365 allows organizations to streamline their IT operations, outsourcing this responsibility to a third-party.

IMPROVE ORGANIZATIONAL COMMUNICATION

Office 365 provides easy access to a set of common tools for employees across the world, eliminating problems caused by some employees having older versions of key productivity tools, or lacking access to them at all. Common communication processes and work approaches can be created to support all employees, and the new tools available through Office 365 – such as Delve and Yammer – provide new ways of cultivating a culture of collaboration.

BUSINESS DRIVERS: SUMMARY

Being clear on the multifaceted business value of Office 365 enables a suitable discussion to be held across all levels of the organization, and for commitment to the big picture value to be embraced. It will also help to prepare employees and executives alike for the short-term migration challenges ahead.

PLANNING THE MIGRATION TO OFFICE 365

Devoting sufficient time, energy, and resources to planning a migration to Office 365 is a critical best practice. A successful migration relies on suitable preparation, sufficient technical knowledge, and a well-executed project plan. Some organizations have migrated to Office 365, only to find they needed to convert back to an on-

premises deployment because of user performance or functionality that was simply not realized. Let's look at some of the aspects involved in the planning phase; this list is intended to be illustrative, not exhaustive.

DOES OFFICE 365 OFFER A COMPLETE SOLUTION?

Office 365 is a single overall brand, but organizations cannot subscribe to Office 365 itself. There are multiple plans with different levels in each plan, and decision makers need to choose the most suitable one for their organization.

- Commercial organizations will need to choose between the Office 365 Business and Enterprise plans. The Business plans support up to 300 users; the Enterprise plans have no such limits. Most enterprise customers should choose the Enterprise E3 or E4 plan, which includes access to the latest versions of the Office suite, as well as a comprehensive set of online services.

- Organizations in the education and government sectors should look at the Office 365 plans and pricing tiers that are available to them. In the education sector, plans are available for students and faculty. In the government sector, specific government pricing is available for the Enterprise plans. Moreover, availability differs by geography.

Organizations can tailor the mix of plans they purchase for employees, noting the specific limitations of each plan, however. For example, if only half of an organization's employees use Office apps regularly, decision makers can create a mixed plan that gives rights to the Office apps for 50% of employees and no rights to the Office apps for the remainder. Equally, and in deference to the idea of clearly evaluating all of your options, in some instances it can be more financially beneficial for an organization to choose one of the cheaper Office 365 plans and use third-party products or services to create an overall solution.

DETERMINE THE STRATEGIC DESIGN DESTINATION

While there are three general approaches to embracing Office 365, practically speaking very few organizations will be able to start afresh under the first general approach of starting again (commonly called a "greenfields" strategy). There is simply too much existing content already in regular use such that rebuilding from the ground up is impossible.

The two remaining approaches are:

- **Office 365 Hybrid**
  Move some or most of the on-premises capabilities to Office 365, but retain some capabilities on-premises. Almost all organizations should retain an Active Directory Server and associated tooling for managing users, but other capabilities for specific purposes may also be retained on-premises over the long-term. For example, SharePoint servers to host older content that is not worth migrating to Office 365 can be retained on-premises, as can email archiving. Organizations with internal business applications that integrate with Exchange, use heavily customized SharePoint setups, and have complex compliance and archiving requirements will want to pursue the hybrid model. Companies with email information on legal hold may be forced to maintain a hybrid configuration indefinitely as there is currently no straightforward way to migrate preserved information from an on-premises server to Office 365.

- **Full Migration to Office 365**
  Move all capabilities to Office 365, retaining next to nothing under an on-premises model (apart from an Active Directory Server). This is the true "all-in" approach to Office 365, with all current and historical data, documents, processes, and activities taking place through Office 365. The migration allows the organization to move all data into Office 365 that can be moved, and to recreate the systems and processes it needs to operate using the tools available

in Office 365. The Hybrid model above will be necessary during the migration process, but the destination design is to decommission all on-premises infrastructure.

For both approaches, there are vendors that offer migration tools to streamline the move to Office 365. These include tools for moving .PST content to Exchange Online, migrating documents from the file share into SharePoint Online or OneDrive for Business, and from various SharePoint document libraries to SharePoint Online. The migration tools streamline the process by respecting key metadata, providing early warnings of file type and file name incompatibilities, and supporting the redesign of an information architecture in SharePoint Online as the site structure is recreated.

Our research found that between 23% and 42% of organizations would employ third parties, such as consultants or vendors' professional services organizations, to assist in the migration process.

There are also vendors that provide cloud-based services that complement either approach to Office 365, for boosting the native capabilities of Office 365 in order to create an enterprise-class service. For example, Office 365 suffered at least one multi-day outage in 2014, causing mail routing problems and undelivered email for many organizations. Complementing an organization's Office 365 plan with a high availability cloud-based email continuity service will bring a much needed disaster recovery route and help assure the business value that organizations are seeking to achieve by shifting to Office 365.

DESIGN A RELIABLE NETWORK INFRASTRUCTURE FOR ACCESSING OFFICE 365

Moving the majority of current data and communications into any cloud-based service – Office 365 included – relies on having highly available, high-speed Internet connectivity. If an Internet link goes down, everyone's ability to access current working documents, communicate through email, and host meetings through Lync is simply gone. Provisioning a reliable network infrastructure may include:

- Securing sufficient Internet capacity for each office building or campus. The actual traffic an organization needs to support will have to be analyzed and managed over time, but it will certainly be significantly higher with cloud-based applications compared to historical requirements when much of the total network traffic was kept inside the organization.

- Considering the acquisition of redundant network links for high priority office locations. Diversity of telecommunications provider and diversity of physical connectivity methods will help assure high levels of service.

- Deciding how to design the firewall topology. Organizations that currently use a centralized firewall topology are likely to find that a decentralized topology provides much better quality-of-service to employees at each office location. Of course, this will have flow-on effects, raising the need for centrally managing multiple firewalls, and having a methodology for keeping the firewall rules consistent across the environment.

In mid-March 2015, Microsoft announced its intent to provide a private network connectivity option to Office 365 called Azure ExpressRoute for Office 365. A private network option already exists for Azure, Microsoft's other cloud service, and this capability will be extended to Office 365 customers later in 2015. Keep in mind the upcoming availability of ExpressRoute as an option in Office 365 planning activities.

IDENTIFYING COMPLIANCE, SECURITY, ARCHIVING AND eDISCOVERY REQUIREMENTS

In planning an organization's migration to Office 365, decision makers will need to evaluate how Office 365 fits with their business and legal requirements for email

security, compliance, archiving, and eDiscovery. They will also have to decide whether to invest in a disaster recovery service to ensure email continuity and end user access.

- **Email Security Requirements**
  Email security covers capabilities like virus filtering, malware detection, spam filtering, email encryption, and data loss prevention. An organization is likely to have a well-established set of approaches to these email security challenges, and they will need to ensure that Office 365 will appropriately meet or enhance the current state of performance. Office 365 offers email security in the form of Exchange Online Protection, with anti-virus, anti-malware, and anti-spam capabilities. Any rules and tuning that organizations have applied to their current email security offerings are unlikely to transfer across to Exchange Online Protection, meaning they will need to start over if they give up their current tools. Many email security vendors offer a dual-layered cloud and on-premises security approach, allowing organizations to continue to leverage their email security investment while migrating to Office 365. These complementary solutions often provide a focus on mitigating advanced threats, such as targeted phishing and advanced malware, further strengthening the overall protection.

- **Compliance Requirements**
  Most industrialized nations have varying degrees of industry-related regulatory retention requirements specifying what organizational data (including email) should be kept and for how long. For example, the United States has records retention laws that potentially touch every business, including retention laws targeted at the financial sector, healthcare, energy, pharmaceuticals, and transportation, as well as general employment laws that span all industries.

  Microsoft has implemented various compliance features into Office 365, including HIPAA Business Associate Agreements, EU Safe Harbor and Model Clauses, FISMA Authority to Operate, and PCI DSS Level One, among others. Some compliance capabilities are not available in Office 365, however, and organizations may need to look elsewhere if they require guaranteed data retention or granular policies, for example. Other compliance principles are maintained differently in a cloud model—such as chain of custody where the document owner is not in direct possession of their documents—and those changes will need to be understood and negotiated with your compliance and legal teams.

  Compliance also extends for many to the way that data is managed and migrated, as well as the need for a full chain of custody. Manual migrations for some industries do not have the industrial rigor or audit trail that they will be able to stand behind and is not always considered legally defensible.

- **Archiving Requirements**
  An organization's archiving requirements are defined by the industry sector(s) in which they operate, the geographies in which they do business, and the business rules they operate under. These are not dictated by Office 365 but must be fully met by Office 365 if the organization is going to rely fully on Office 365. Many archiving vendors offer complementary capabilities to Office 365, so that organizations can continue to use proven archiving tools and approaches after migrating to Office 365. For example, if an organization needs archiving capabilities not available in Office 365 – such as eDiscovery workflow, batch search, and broader support for indexed file types – they should evaluate using a third-party cloud-based or on-premises archiving solution in conjunction with Office 365. More information on this topic is available in a white paper that Osterman Research published in March 2015.

  A word of warning: do not assume that archiving capabilities are the same between on-premises servers and Office 365 services. For example, Lync Online does not archive conference content, conference whiteboards, and conference

polls, whereas Lync Server does. Some capabilities are different (read "lost" and "gained") in moving from servers to services, and decision makers will need to understand both of these prior to migration.

Finally, when moving from a legacy archive to any new archive—Office 365 or otherwise—the organization must understand in detail the attribute mapping between the two archive solutions. If attribute mapping is not done correctly, the data in the legacy archive will become corrupted and will no longer be a true and complete record of historical actions, thereby breaking the chain of custody that so many firms require.

- **eDiscovery Requirements**
  There are many situations when organizations need to be able to search and discover emails and other electronically stored data. Situations include but are not limited to Early Case Assessment for litigation, information access requests, and internal HR investigations. Any data that is identified to be relevant or potentially relevant to the situation must be held under special safeguards, including deletion prevention. Office 365 includes some eDiscovery capabilities, but they are limited. One significant limitation is that in order to identify BCC and distribution list recipient information, a mailbox must first be placed under legal hold. In other words, in order to discover who sent and received a message, all mailboxes would have to be on hold and all mailboxes would have to be searched all the time. This could make the eDiscovery process slow, unreliable, and prone to false positives leading to the capture of too much data to review and the cost associated with that.

- **Disaster Recovery Requirements**
  Office 365 has been architected to deliver a highly available set of services. It is, however, still prone to failure, and the Exchange Online outages of 2014 and earlier ring the warning siren. Since email is mission-critical to almost every organization, increasing the disaster recovery capabilities to ensure email service continuity is a worthwhile investment. For example, third-party services are available to spool inbound email for Exchange Online for the times when Exchange Online is offline. Some services give users alternative means of accessing their email under such circumstances, and the services will bring Exchange Online back up-to-date once service is restored. In selecting an email continuity service, ensure it is protected against advanced threats so that the continuity data store is not compromised or used as an attack vector.

- **Backup Requirements**
  Microsoft will backup all content in Office 365, but decision makers may decide to keep a separate backup as part of good IT governance processes and peace of mind. Either a hybrid deployment of on-premises and Office 365 is necessary to make this happen, or the use of a third-party cloud-based archiving service, which will create a backup copy of data in a separate location.

EVALUATE THIRD-PARTY TOOLS WITH OFFICE 365

Office 365 offers a broad set of widely applicable, general-purpose tools and capabilities, but it is not a complete solution. Third-party tools and services can be added to Office 365 to mitigate unwanted design choices, provide a multi-year consistency of approach, and extend Office 365 with greater richness. Organizations need to evaluate third-party tools to support their use of Office 365:

- **Dial-In Audio Conferencing**
  Lync Online does not include dial-in audio conferencing capabilities. Organizations need to acquire such services from a certified partner.

- **Workflow Design and Execution**
  Designing standard processes – with exception loops and escalation pathways – provide a means of driving consistency, efficiency, and compliance. Add-on workflow design tools and execution engines are available for Office 365.

- **Content Migration**
  Tools for efficiently moving content to Office 365, and repurposing it across the various services, while retaining metadata integrity and access rights.

- **Apps for Tablets and Smartphones for End Users**
  Many vendors offer apps for accessing Office 365 from tablets and smartphones, as well as computers. These often support a richer interaction experience, and enable offline access through seamless synchronization.

Microsoft also offers a set of certified add-on tools through the Office Store. It is worth reviewing the catalog to see what is available for Office 365.

IMPLEMENT THE ON-PREMISES REQUIREMENTS FOR MIGRATING TO OFFICE 365

A final activity in an organization's planning phase is to ensure they meet the on-premises requirements for migrating to Office 365. Three key requirements are:

- **Active Directory**
  Having an on-premises Active Directory server. This is used for migrating and managing user accounts during the migration process, and supporting single sign-on for employees accessing both on-premises servers and Office 365 services.

- **Pre-Migration Upgrades**
  Installing the required operational versions of Exchange Server, SharePoint Server, and Lync Server, along with any pre-migration co-requirements. Migrating from older servers to Office 365 may require an intermediate upgrade in order to attain the required minimum standards.

- **Internet Capacity**
  Provision sufficient Internet capacity. Migrating current, historical, and legacy data to Office 365 will involve shifting many terabytes of data off-premises and into the cloud, and organizations will still need to continue standard business operations at the same time. Whatever is in place at the moment will most likely be insufficient. An alternative approach is to select a third-party archiving service that accepts legacy data in physical form—such as hard drives and other digital storage media—for upload into the archive. This will greatly reduce the volume of legacy data that has to be moved over the wire to Office 365, shrinking the migration time frame and reducing the risk of data loss.

With the proper foundation in place and a solid migration plan to go with it, organizations are approaching readiness for the actual migration.

MANAGING THE MIGRATION PROCESS

Once an organization has completed its pre-migration activities and developed and tested a plan for moving to Office 365, it is time to start executing on the plan. In this section we will explore a number of best practices for managing the migration process.

ADDRESS EXCHANGE MISCONFIGURATION

Although Exchange Servers may be working adequately, migrating to Exchange Online is likely to highlight any hidden problems. IT will need to be prepared to address any stability, mailbox corruption, and misconfiguration problems with Exchange that arise during the migration. For example, some Exchange mailboxes may contain corrupted messages, and the migration of these to Exchange Online is going to cause problems. It is better to address these problems prior to migrating the user and their mailbox to Exchange Online. IT may also uncover problems with firewalls, proxy devices, and other boundary protection approaches that will need to

be addressed during the migration.

ESTABLISH ADVANCED EMAIL SECURITY FOR EXCHANGE ONLINE

Given the havoc a successful virus or malware attack can unleash on an organization, Osterman Research has long advised clients to invest in dual layers of email security: one in the cloud, and one on-premises. With Exchange now shifting to the cloud in Office 365, the advisory still stands, but with dual cloud layers. Screening email for advanced threats—such as polymorphic malware, malicious URLs, and malicious attachments in the form of zero-day threats—prior to routing it to Office 365's own email security services will greatly assure a cleaner mail flow and the removal of any attack vectors. With the continued escalation of attack methods, advanced protection is required that can emulate user and browser activity, provide per-user insight for threat remediation, and offer detailed reporting for post-infection clean up activities.

MIGRATE CURRENT AND ARCHIVED EMAIL CONTENT INTO EXCHANGE ONLINE

Moving to Exchange Online is rarely a greenfields situation; users have much of their digital lives contained in their mailbox, as well as reminders about future events like meetings and tasks to complete. This data needs to be moved into Exchange Online with as little impact on users as possible, and indeed Microsoft offers standard ways for cutting users over from Exchange on-premises to Exchange Online under a hybrid migration scenario. For example, as shown in Figure 3 on the next page, the vast majority of organizations will want to migrate existing .PST files into Office 365, but other content types will also need to be migrated, as well.

There is, however, a set of related activities that will need to be managed:

- **Prune Content from Exchange**
  If current Exchange Servers are storing messaging data that is no longer required for current business purposes, archiving the data out of Exchange prior to migration is a good approach. This will reduce the time and expense of migrating to Exchange Online, and will give everyone a cleaner starting point with the new service.

- **Locate and Deal with .PST Files**
  Users have historically worked around mailbox size quotas by using local .PST files to offload their main mailbox with messages they want to retain. It is unlikely that IT can just delete these .PST files because they contain business-relevant information that will be subject to compliance and legal requirements. And, Microsoft offers no supported tool or practical method for migrating content from .PST files into Office 365, and also does not support the use of .PST files with Office 365, so IT cannot move the .PST file to Exchange Online. Third-party vendors, however, offer migration tools for the automatic discovery of .PST files on their corporate network, and the managed migration of content into Exchange Online.

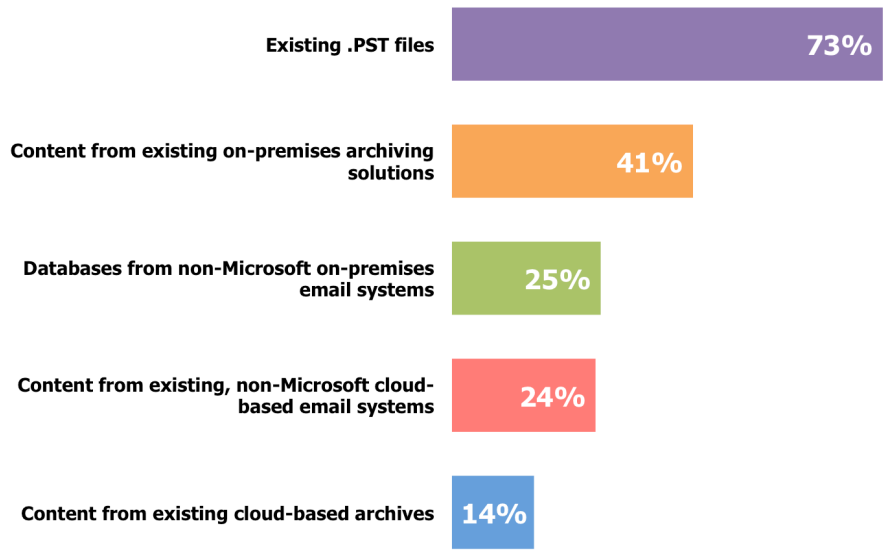
- **Migrate or Retain Archiving Data**
  Depending on what IT chose regarding email archiving during their pre-migration planning activities, they either migrate historical archive data into Exchange Online Archiving or configure Office 365 to keep using their current archival system or a cloud-based archival service. They will almost certainly need to use third-party tools for migrating archival data into Exchange Online Archiving if they decide to take this route in order to protect the chain of custody. Moreover, they may need to undertake a similar migration activity if they migrate to a third-party archival cloud service, but if their migration is from the on-premises server version of an archival product to the same vendor's cloud-based service, the migration should be more streamlined.

- **Identify Data on Legal Hold**
  IT will need to identify any data currently on legal hold and exclude it from the migration process; while this data may ultimately be uploaded to Office 365 specific steps must be taken and documented to ensure it was preserved and no metadata was altered during the migration process.

- **Migrate or Archive Inactive Mailboxes**
  Many organizations have a regulatory or business requirement to retain mailbox data of departed employees. One option is to use the Office 365 Inactive Mailboxes capability to migrate mailbox data from on-premises Exchange 2010 or 2013 to Office 365. This requires a subscription for the departed employee during the provisioning and data import process, but not after the data has been migrated and the mailbox marked as inactive. An alternative option is to move the inactive mailbox from on-premises Exchange 2010 or 2013 into a third-party archive.

As organizations move to Exchange Online in Office 365, they want to ensure that they have taken all of the required data along on the journey. It is essential not to unintentionally leave unmanaged or orphaned data lying around on the corporate network.

Figure 3
Content Sources that Organizations Will Want to Migrate to Office 365



Source: Osterman Research, Inc.

INSTITUTE ADVANCED SECURITY FOR FILE SHARING

As organizations increase adoption of SharePoint Online and OneDrive for business, users will use these systems to share files in place of email. A zero day threat can use collaboration systems to travel throughout your organization or even to/from customers or partners with whom you share files. Advanced security controls can integrate with SharePoint Online and OneDrive to discover and prevent the spread of advanced threats.

MIGRATE OTHER CONTENT INTO THE APPROPRIATE DESTINATION IN OFFICE 365

As noted earlier in this white paper, migrating to Office 365 is a significant undertaking, due to all of the major activities involved, and also the opportunity it affords to think some of the ways an organization uses file shares, SharePoint, and Lync. Decision makers will need to migrate existing content from their current systems into the appropriate place in Office 365. This will include:

- **Migrate My Documents to OneDrive for Business**
  Most of the documents and files in the My Documents or Documents folder structure for individual users is best shifted into their OneDrive for Business area. OneDrive for Business provides corporate-provisioned file sync and share service for individuals, and allows for sharing of files directly with other people. Once an individual's files and documents are in OneDrive for Business, they will be able to access and work on them from multiple devices – laptops, tablets, and smartphones.

- **Migrate Other Content from My Documents to SharePoint Online**
  Some of the documents and files stored in an individual's My Documents or Documents folder represent team- or project-related content that should be shifted to a document library in a site in SharePoint Online. Users will need guidance on where to shift these files and documents.

- **Archive Unnecessary File Share Content**
  There is little value to be gained by moving out-of-date file share content to Office 365. IT should definitely migrate the current and well-used files and documents and, if possible, should trash any documents that are no longer required (subject to compliance limitations). Most organizations would benefit from an audit of the usefulness of the folders and documents on their file share prior to moving to Office 365, and archiving whatever is not required or no longer necessary prior to the shift. Due to the differences in how versions are managed on a file share compared to the advanced approaches in SharePoint Online, IT may be able to archive more than one-half of the documents on their file share. Migrate the most current version and archive the rest.

- **Migrate File Share Content into SharePoint Online**
  Much of the shared documents and content on file shares should be migrated into SharePoint Online. Note that there are limitations on the type, size, file name length, and number of files that can be stored in a document library in SharePoint Online. If organizations used a third-party tool during their pre-migration planning activities to assess the validity of their current files to work with SharePoint Online, they can proceed in light of that report card and any warnings. If they do not know what will and won't work with SharePoint Online, they will need to undertake that analysis now. Practically speaking, IT will need to invest in a third-party migration tool to shift file share content into SharePoint Online while maintaining key metadata and chain-of-custody information.

- **Migrating Intranet Content to SharePoint Online**
  If an organization currently uses SharePoint on-premises to power its intranet and you are going to migrate this to SharePoint Online, then migrate across the content that can be moved. Note that SharePoint Online has limits on the customizations and approaches that work perfectly in SharePoint on-premises, so IT is very likely to have to recreate the organization's intranet on SharePoint Online – respecting its particular capabilities and boundaries – rather than migrating their intranet as such. Use of a third-party tool to help with the migration of content they can move is highly recommended. If an organization currently uses a different intranet toolset on-premises and are going to move their intranet to SharePoint Online, they have quite a project ahead of them.

- **Migrating Workflow Processes to SharePoint Online**
  The ability to craft custom workflows for handling documents, requests, and other activities is a well-established capability in SharePoint on-premises. There are some differences in what decision makers can effectively do in SharePoint Online, and they are very likely to find themselves re-creating workflow processes in the new environment. Some third-party vendors offer workflow design and execution engines that work both on-premises and in conjunction with Office 365, but even those tools must respect the built-in security boundaries in Office 365. For example, unless an organization has a hybrid deployment of SharePoint, getting a workflow process to interrogate a non-Office 365 system or server will be more difficult compared to when everything was running on-premises.

- **Rethinking Customizations to SharePoint**
  SharePoint on-premises gives the organization complete control over customizations; SharePoint Online does not. Customizations that organizations have created on-premises will need to be re-imagined for SharePoint Online, or IT will need to maintain a hybrid deployment of SharePoint to get around such design limitations.

- **Migrating Collaboration Content to SharePoint Online or Yammer**
  Current project spaces and associated content in SharePoint will need to be migrated to a new project space in SharePoint Online, or if Yammer is going to feature heavily in an organization's work, into Yammer. As with moving file share content, practically speaking IT will need a third-party tool to facilitate these migrations.

- **Migrating to Lync Online**
  In a Lync Hybrid deployment, some users can be supported by Lync on-premises and others by Lync Online. Users can be migrated to Lync Online when the conditions are right. Note that only 200 entries per contact list are migrated from Lync Server to Lync Online, and any meetings and voice configuration data from Lync Server is not migrated to Lync Online. Users will need to re-establish their meetings, and voice configuration and services worked out through an agreement with a certified Lync Online partner.

There will be other activities required to migrate current content into Office 365, and a training program and adoption strategy prepared to help users make the most of the new capabilities. The activities above will help minimize the pain of the migration, by giving users as much of their current data and documents as possible.

SUMMARY

There are four key issues with which organizations must contend as they consider a migration to Office 365.

- Understand that migrating to Office 365 is a significant undertaking for many organizational stakeholders, including the IT department, the security group, and compliance and eDiscovery teams, among others.

- Be clear on the business drivers for migrating to Office 365.

- Decision makers will need to plan their migration to Office 365, taking into consideration the multifaceted requirements of many stakeholders.

- Moreover, they will need to manage the migration process itself.

SPONSOR OF THIS WHITE PAPER

ABOUT TREND MICRO

www.trendmicro.com
@TrendMicro
+1 888 762 8736
+1 817 569 8900

Trend Micro™ Cloud App Security enhances Office 365 email, SharePoint Online, and OneDrive for Business with advanced threat protection. The solution extends Office 365 built-in security with sandbox malware analysis to detect zero-day malware and malicious code hidden in PDF or Office documents. Cloud App Security simplifies setup by integrating directly with Office 365 using an API.

Keep collaboration free from infiltration

- Prevents criminals from using SharePoint or OneDrive to migrate between partners or within an organization using malware disguised as ordinary office documents.
- Ensures files uploaded from mobile devices without full security controls are scanned for threats

Block zero-day and hidden malware

- Enhances the static antimalware scanning included with Office 365 with dynamic sandbox malware detection to lower your risk of breach.
- Detects malware hidden inside documents using document exploit detection

Seamlessly extend Office 365 security

- Direct cloud-to-cloud integration via Microsoft API enables high performance and while eliminating the need to re-route email.
- Works with all devices, including desktops, mobile devices, or Outlook Web Access with zero impact to Office 365 user and administrator functionality

Trend Micro is a Microsoft Gold Certified Partner who has protected Exchange and SharePoint systems for over 15 years. Trend Micro enables the smart protection of information, with innovative security technology that is simple to deploy and manage, and fits an evolving ecosystem. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™ infrastructure, and are supported by more than 1,200 threat experts around the globe. For more information visit www.trendmicro.com/office365