WHITE PAPER

How to More Thoroughly Protect Email in Exchange Online

An Osterman Research White Paper

Published June 2016

FORCEPOINT
POWERED BY Raytheon

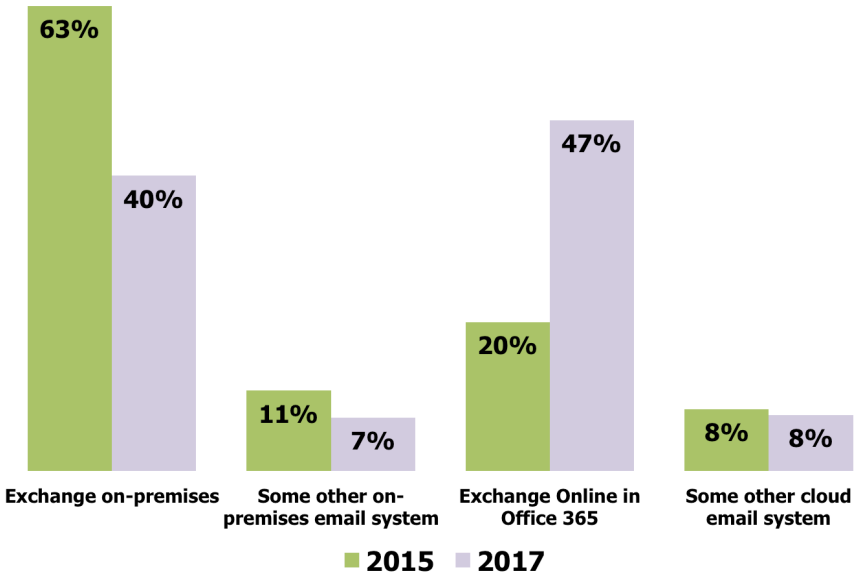
OSTERMANRESEARCH

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

Microsoft has been marketing remotely hosted/cloud-based versions of Exchange and other elements of its Office suite for many years, but has gained serious traction with the current iteration of this effort – Exchange Online and Office 365™. As shown in Figure 1, a substantial proportion of organizations whose users are today served by on-premises versions of Exchange will be served by some version of Office 365, whether email only through Exchange Online or by some combination of elements offered within Office 365.

Figure 1
Distribution of Users by Platform, 2015 and 2017



Source: Osterman Research, Inc.

There are several important points presented in this white paper, the focus of which is Exchange Online:

- Exchange Online is a robust and capable offering that can significantly reduce an organization's cost of providing email and collaboration services to its users. Even large enterprises can realize significant cost savings and other benefits from the use of Exchange Online.

- However, as with many cloud-based applications, there are limitations with the security capabilities provided along with Exchange Online. For example, the DLP capabilities are less mature and less capable than what are available from some other enterprise DLP solution vendors, there are limitations in the filtering of spam and malware, limitations in detecting and remediating targeted and more advanced threats, and a more difficult experience for mobile users and for those who rely on encryption.

- Consequently, enterprise decision makers migrating to Exchange Online should evaluate and seriously consider the use of third-party email security, advanced threat detection and data loss prevention solutions to supplement or replace the security services available from Microsoft for Exchange Online and Office 365.

ABOUT THIS WHITE PAPER

This white paper was sponsored by Forcepoint – a brief overview of the company and its relevant offerings is included at the end of this document.

AN OVERVIEW OF EXCHANGE ONLINE AND OFFICE 365

THE SHIFT FROM CAPEX TO OPEX

Migration of communication and collaboration services to the cloud offers a way to gain access to communication and collaboration services without incurring the capital expenses necessary to build or expand an on-premises environment, nor accepting the responsibility and related costs of managing the resulting on-premises infrastructure. Exchange Online is essentially a rented cloud service and key infrastructure elements are not owned or managed on-premises. That is neither good nor bad, but simply a different way of thinking about shifting the mindset from acquisition costs (CAPEX) to licensing fees (OPEX).

There are pros and cons associated with this shift. Among the benefits of operating internal infrastructure is the ability to bypass one or two upgrade cycles and thereby avoid the costs of migration from one version of Exchange (or some other platform) to another. However, once an organization has migrated its users to Exchange Online, that option is no longer available. The upside, however, is that software is continually up-to-date and current with new standards and file formats. Consequently, by deploying Exchange Online, organizations can realize the benefits associated with the migration to new capabilities without incurring the problems of the migration process.

OFFICE 365 OVERVIEW

Office 365 includes a number of offerings, some or all of which are offered in some or all the various plans offered by Microsoft[i]:

- Exchange Online: Business-grade email, calendaring and scheduling functionality with a 50-gigabyte mailbox. Exchange Online can also be purchased as a standalone application.
- Full copies of Microsoft Office applications, including Word, Excel, PowerPoint, Outlook, Publisher and OneNote on up to five PCs or Macs.
- Microsoft Office available on up to five mobile devices.
- Online versions of Word, Excel and PowerPoint.
- One terabyte of storage per user with Microsoft OneDrive for Business.
- SharePoint Online.
- Skype for Business, which includes voice, instant messaging and videoconferencing capabilities.
- Social media capabilities using Yammer.

Office 365 includes a variety of other tools and capabilities, including corporate intranets, business intelligence tools, Office Graph, group policy tools, a corporate video portal, and various compliance tools.

Pricing for Exchange Online is $4.00 or $8.00 per user per month (before discounts)[ii], Office 365 plans are priced at anywhere from $5.00 (Office 365 Business Essentials) to $35.00 (Enterprise E5) per user per month[iii].

SECURITY IN EXCHANGE ONLINE AND OFFICE 365

Microsoft offers a number of security services in conjunction with Exchange Online and Office 365:

- Exchange Online Protection (EOP), available for $1.00 per user per month, offers protection against spam and malware. EOP uses multiple anti-virus engines that Microsoft guarantees will protect users from all *known* viruses and 99% of spam[iv].

- Exchange Online Advanced Threat Protection (ATP), available for $2.00 per user per month, offers protection from more advanced threats like malicious links and suspicious attachments. ATP offers reporting about the types of threats that have been intercepted and the individuals in an organization that are being targeted[v].

- Data Loss Prevention (DLP) in Exchange Online are policies created in Exchange Administration Center that are comprised of transport rules, actions and exceptions applied to email messages and the attachments they contain. DLP is available only in the Office 365 Enterprise E3 and E5 plans[vi].

- Azure Rights Management (RMS), the cloud-based version of Active Directory Rights Management Services, is a set of identity, encryption and authorization policies designed to protect email and files. RMS supports Office 365, but also other Microsoft offerings, including on-premises version of Exchange and SharePoint, and Office 2010 through 2016[vii].

EXCHANGE ONLINE SERVES VARIOUS MARKETS

Microsoft offers Exchange Online in a variety of plans, at a number of price points, and tailored for several different markets: enterprise, government and educational institutions. An advantage of Office 365, as with any cloud-based messaging or collaboration solution, is the ability to mix and match plans to suit various groups within an organization. For example, full-time information workers can be outfitted with a full suite of Office 365 solutions, while temporary workers, occasional workers, or those who work in the field can be enabled with a less capable/less expensive plan. This can significantly reduce communication and collaboration costs in an organization compared to the traditional, on-premises delivery model.

WHY ARE ENTERPRISES SHIFTING TO EXCHANGE ONLINE AND OFFICE 365?

Exchange Online, as well as other cloud-based communication and collaboration solutions, can lower the costs associated with providing these capabilities in various ways:

- **Lower infrastructure costs**
  An important way that Exchange Online can reduce the cost of ownership for communication and collaboration capabilities is by eliminating the majority of the up-front costs associated with deploying new systems. For example, a fresh deployment of Microsoft Exchange or an upgrade from one version of Exchange to another can be expensive because of the need to purchase servers, software, appliances, and the other infrastructure elements necessary to support it. By using Office 365, most of these expenses are eliminated. Of course, most of the desktop and/or mobile infrastructure costs must still be incurred regardless of the delivery model, but these represent only a fraction of the total cost of ownership for deploying a new system.

  Another important advantage of migrating to Exchange Online is the ability to reduce the ongoing costs of ownership associated with communication and collaboration. For example, an on-premises deployment of Exchange Server would necessitate periodic upgrades of hardware as new users are added to the system, additional servers or appliances are added to deal with new threats, etc. These costs are eliminated when using Exchange Online.

- **Reduced labor costs**
  Another important benefit of Exchange Online is its ability to do away with most

IT labor costs. For example, in the typical Exchange-enabled organization, a full-time equivalent (FTE) IT staff member can support roughly 500 to 1,500 users, depending on the size of the deployment, the capabilities available to users, and other factors. Using Exchange Online, however, a single IT staff member can support many times the number of users. For example, if we assume that an Exchange Online or Office 365 user in an organization will require 30 minutes of support per year (an overly large estimate for most organizations), then an FTE IT staff member working 2,000 hours per year will be able to support 4,000 users.

Using the figures in the paragraph above, and assuming that the fully burdened annual salary of an IT staff member is $75,000, the on-premises labor cost to support Exchange will be anywhere from $50 to $150 per user per year. The annual labor cost for Exchange Online or Office 365, on the other hand, will be just $18.75.

- **Problem shifting**
  Another key benefit of Exchange Online and Office 365 is "problem shifting": i.e., the problems of crashed servers, faulty storage, power interruptions, application faults, failed backups, corrupted data stores, and other problems are transferred to Microsoft and are borne by their data center infrastructure and staff members. The result is a shift of problems away from customers – the organizations that provide Exchange Online to their users – and to Microsoft who are arguably better equipped to deal with them. This can reduce the cost of ownership for communication and collaboration, and is one of the primary reasons that IT staff members can support so many more users in an Exchange Online environment.

  It is essential to note a couple of things. First, while email-related problems are shifted to Microsoft, users will continue to hold IT responsible for email outages and other problems, and so organizations that deploy Exchange Online will still need to deal with these issues. Second, an enormous opportunity created by problem shifting, and the resulting freeing up of IT staff time that was formerly devoted to managing on-premises infrastructure, is that IT can devote more attention to issues like insider threats, how and where sensitive information is being stored, and other pressing issues.

- **Cloud-first benefits**
  Another reason that many organizations are adopting Exchange Online is their desire to stay on the Microsoft roadmap. Microsoft is now, for all intents and purposes, a "cloud-first" vendor: new features and functions are introduced first to Exchange Online customers and only later to customers who purchase on-premises solutions.

- **Allocate scarce IT resources to strategic initiatives**
  Managing email and collaboration systems using on-premises infrastructure and in-house staff rarely provides a competitive advantage of any kind. Consequently, many decision makers are realizing that they can achieve greater returns from their IT staff investments by shifting non-strategic activities to the cloud, while using IT staff for activities of more strategic importance.

RECOMMENDATION

Decision makers should seriously consider the use of Exchange Online. Microsoft's own numbers show that as of late 2015 there are more than 60 million active Office 365 users in the commercial space and more than 18 million consumer subscribers[viii]. Exchange Online and Office 365 are good offerings with a large number of features that are being improved and updated on a regular basis. Moreover, they are offered by a large, profitable and financially stable company that is now fully committed to the delivery of its offerings through the cloud first.

CONSIDERING THE SECURITY LIMITATIONS

Email security is an essential consideration for any organization and should be a top-of-mind priority for every decision maker focused on communication and collaboration. Capabilities like spam and virus filtering, malware detection, email encryption, advanced threat detection, and data loss / data theft prevention are important considerations as part of an effort to protect corporate intellectual property, customers' personal data, and other kinds of sensitive and confidential data. Moreover, robust security is an essential element of good information governance and the ability to comply with legal, partnership and regulatory obligations.

Most organizations have a well-established set of approaches to these security challenges for their on-premises Exchange deployments, and they will need to ensure that their security services for Exchange Online will meet or enhance the current state of performance. Microsoft offers email security services in the form of EOP, ATP, DLP and RMS, as discussed above.

RECONFIGURING POLICY AND SECURITY CONTROLS

Any rules and tuning that organizations must apply to their current email security offerings are unlikely to move 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 leverage their email security investment while migrating to Exchange Online. These complementary solutions often provide a focus on mitigating advanced threats, such as targeted phishing and advanced malware, further strengthening the overall protection.

Exchange Online and Office 365 include a number of useful security features, but there are a number of situations in which these capabilities will not satisfy many enterprise security requirements. For example:

- **Limited DLP capabilities**
  While security in Exchange Online tends to be more focused on inbound threats, Microsoft offers DLP capabilities, including pre-configured policy templates for a variety of scenarios, such as data subject to the Gramm-Leach-Bliley Act or PCI-DSS[ix]. For example, the DLP Policy Tips capability in Office 365 will warn users who are about to send sensitive or confidential information in an email that some of the content may be in violation of corporate policy. However, this capability does not work with all versions of Outlook, and users can still override the warnings presented to them. While DLP Policy Tips is useful, it generally serves as more of a guide for educating users about corporate policy than as a capability that will prevent the distribution of sensitive or confidential information through email. Some of the limitations of DLP in Exchange Online include:

  - Lack of data fingerprinting and basic detection capabilities.
  - Limited policy coverage for compliance and protection of Personally Identifiable Information (PII) and intellectual property.
  - Lack of a DLP incident queue.
  - Lack of incident workflow support.
  - Reporting is basic and does not offer customization.
  - No role-based access control.
  - DLP for SharePoint and OneDrive require the use of separate management consoles.

Moreover, data leakage can occur through file share and sync solutions, such as Microsoft OneDrive, if sensitive or confidential content is not protected or blocked from storage in these solutions. Many third-party solutions are better at protecting against data loss through these tools.

- **Lack of support for redundant or more sophisticated spam filters**
  Exchange Online offers basic spam filtering capabilities, but not at a level that many enterprises will require to protect their users from the variety of spam and spam-like content they are very likely to receive in their inboxes. (One source estimated that 3% of spam is able to successfully penetrate Exchange Online Protection's anti-spam defenses[x].) For example, Exchange Online spam filtering is based on relatively static spam filtering capabilities that do not provide capabilities to reliably detect phishing and spearphishing attacks. There are no reliable capabilities to detect and filter "graymail" – i.e., valid content, such as newsletters, that users no longer want to receive. Moreover, the spam quarantine capabilities in Exchange Online are decentralized and will too easily permit users to release a validly quarantined spam email that might contain malicious content.

- **Limitations for targeted and more advanced threats**
  Standard Exchange Online threat protection – available as part of Exchange Online Protection – is not as sophisticated or as broad-based as that offered by some third party providers. To remedy this, Microsoft introduced Exchange Online Advanced Threat Protection 2015 for an additional fee[xi] (included as standard only with the E5 plan), which includes protection against malicious URLs, URL trace capabilities and protection against zero-day threats and other unknown malware variants.

  However, Advanced Threat Protection relies solely on sandboxing (an isolated virtual machine in Azure) as the only option for managing unknown or potentially suspicious attachments. While allowing suspect attachments to run in a sandbox can be useful and is a recommended best practice, this can create an excessive number of false positives (attachments identified as malicious when they are not), and it can result in significant delays in email delivery. To the latter point, Microsoft anticipates that the typical delay will be no more than 10 minutes[xii], but can extend to as long as 30 minutes (the service-level agreement) when a timeout is reached. Moreover, some sophisticated threats will recognize that they have been sandboxed and will remain dormant until they reach the recipient's inbox.

- **Limitations around reporting for response to threats**
  Granular segmentation in a quarantine is essential to distinguish between phishing and spam. However, phishing attempts and spam are mingled in Exchange Online as a result of there being only two queues for inbound email: malicious attachments and spam. There should be a third queue for phishing attempts to provide more granular management of malicious inbound content.

  Exchange Online does not provide a quarantine for outbound email, and so administrators do not have a queue available to them for outbound DLP management. Some third-party security solutions enable outbound filtering based on IP or domain restrictions, as well as user authentication, to prevent malicious, sensitive or confidential content from being sent. Moreover, there are limitations on the support included in Exchange Online for dealing with emails that contain malicious links. Scanning for malicious content is not based on the same level of deep scanning that is available with some third party solutions. A best practice is to configure Exchange Online to relay all outbound email to a third-party security solution for additional and more advanced filtering.

- **Limitations on visibility into message flow for NDRs**
  Some spammers will use forged email addresses in the return-path headers of their messages. When an email server receives such a message for a non-

existent user, it can return the bounce message to the forged address, resulting in what are known as non-delivery reports (NDRs), or "backscatter spam". This type of traffic can represent a significant nuisance for the affected organizations, since it creates bogus traffic that must be processed by a company that never sent the original messages. There are limitations on the visibility into NDRs in Exchange Online that are more capably addressed by some third-party solutions.

- **Limitations on email encryption capabilities**
  Microsoft Azure Rights Management includes Office 365 Message Encryption as an option (at a surcharge of $2.00 per user per month) and is included with the Office 365 Enterprise E3 and higher plans. Encryption in Office 365 is useful, but there are some limitations that decision makers should consider. For example, users cannot revoke access to documents, they cannot track document usage, support for iOS and Android users is available only through an app (which some IT departments will not allow users to download), key encryption options (e.g. S/MIME and PGP) are not supported, and new recipients of an encrypted message must create a Microsoft account and thereby provide sensitive information to read the message. Moreover, encryption in Office 365 uses only a single delivery method (inclusion of an encryption HTML file in a clear text message pushed to the mailbox), but users must be online to decrypt the message because authentication is against the Office 365 service. Also, there is no facility for sending bulk emails, nor is there audit or compliance reporting.

The bottom line is that Exchange Online offers a set of useful security capabilities, but it has limitations that can lead to security breaches, loss of intellectual property, a failure to satisfy regulations, and the need to publicly disclose losses of customers' data without adequate security controls in place.

Security is not Microsoft's primary area of expertise, and so its security offerings may be considered as better suited to the needs of small and mid-sized businesses than enterprises.

WHAT TO LOOK FOR IN AN ENTERPRISE-LEVEL EXCHANGE ONLINE SECURITY SOLUTION

When seeking a security solution – or a set of solutions – to protect enterprise-level Exchange Online deployments, there are a number of important capabilities that should be on the short list as decision makers perform their due diligence when evaluating different vendors' offerings:

- **Outbound data loss prevention is just as important as inbound malware filtering**
  Any security system must protect an organization's data assets from being unintentionally divulged or stolen by unauthorized parties, and so data loss prevention for outbound content must be given equal weight with inbound filtering of malicious content.

- **Mature DLP capabilities are essential**
  Robust and highly capable DLP capabilities are absolutely essential for any business IT environment because DLP impacts every function in an organization: it enables more secure communications, improves compliance-readiness, and it significantly mitigates corporate risk by reducing or eliminating compliance violations, data breaches and related types of problems. Moreover, DLP needs to be implemented everywhere in an organization: in email, for mobile users, on the web, in social networks, etc.

  While Exchange Online provides DLP capabilities, as discussed above, these should be considered relatively basic and limited, and not sufficiently mature to meet enterprise-level demands in most cases. In order to qualify as "enterprise-

level", Osterman Research believes that a DLP solution should include the following capabilities:

- A large set of standard, pre-defined policies covering the broad spectrum of PII, intellectual property protection and compliance protection. These policies must satisfy the demands of all jurisdictions in which an organization operates.
- Data fingerprinting to precisely identify the data to be protected, which in turn translates to significantly reduced false positives. Less precise data definition techniques, such as keyword matching and regular expressions, can result in significant false alarms and even result in policies being disabled.
- DLP incident queue and incident workflow capabilities for security to review and remediate security risks.
- The ability to identify every potential type of content that might violate a corporate, legal or regulatory policy in an email, file, instant message, web application or other communication type or document.
- Robust policy management capabilities that will enable policies to be created and managed for all communication and content types to protect all sensitive content regardless of format.
- DLP capabilities that are integrated across the entire suite of Office 365 applications, including Exchange Online, SharePoint and OneDrive, as well as third party applications.
- Role-based access controls to ensure only a limited and approved audience have access to the sensitive audit information and other content exposed in DLP repositories and incident data.
- Data fingerprinting for unstructured information (databases and tables) is critical to protect customer PII and sensitive data from operational systems (CRM, ERM, ordering systems, etc.)
- Email workflow remediation distributes remediation decisions to data custodians and owners and allows them to decide remediation actions with a simple email response.
- The ability to detect and remediate data theft of small amounts of data over prolonged periods of time that might go under the radar. This is a common technique to circumvent DLP solutions that cannot recognize these slow data leaks.
- Robust reporting capabilities that will enable administrators to create customized reports to monitor results specific to their business and demonstrate results to their executive stakeholders.
- A mature DLP solution must also be able to monitor for data leaks through images, since employees or cyber criminals can take a screen shot or capture an image of sensitive or confidential data in an effort to bypass traditional DLP solutions. An optical character recognition (OCR) capability is an important component of DLP when dealing with images, since it can "read" content in images to prevent data loss.

- **Proper protection for outbound content is essential**
  So, what defines "proper" protection for outbound content? While some DLP solutions will allow content to be sent with sensitive or confidential information redacted from it, this is not the best approach. For example, redaction does not

educate senders about the dangers of sending sensitive information through email or other unprotected channels, and redaction can still reveal at least the *context* of the sensitive or confidential information, if not its *content*. If and when redaction is necessary, a DLP solution should block only the sensitive information contained with a communication or document.

However, instead of redaction, Osterman Research believes that a mature DLP solution should automatically encrypt sensitive or confidential information, quarantine it for review by a compliance officer or supervisor, or simply block it from being sent. The user should be alerted that they are taking an insecure action and given a chance to communicate safely or completely protect data and context with encryption.

- **Maintaining an outbound quarantine**
  An important element of a mature DLP solution is an outbound email quarantine. This allows outgoing email to be blocked based on pre-established policies so that inappropriate content, sensitive data, confidential information, protected health information, PII, customer records and other content cannot be sent in violation of compliance rules. The advantages of maintaining an outbound quarantine include preventing the loss of sensitive or confidential data as shown in the examples above, but also helping to prevent an organization's domain from damage to its reputation or even being blacklisted.

- **Easy-to-use push and pull encryption tools**
  Exchange Online and Office 365 offer only pull encryption via Rights Management Services, but many organizations will want both push and pull encryption capabilities depending on how they want to distribute sensitive or confidential information. Push encryption involves encrypting sensitive content and sending it in a message like a normal email, while pull encryption requires recipients to log into a portal to retrieve encrypted messages. Both are important capabilities to offer to users, since push solutions are inherently more convenient for recipients, but pull solutions enable the sender to maintain more control over the encrypted content.

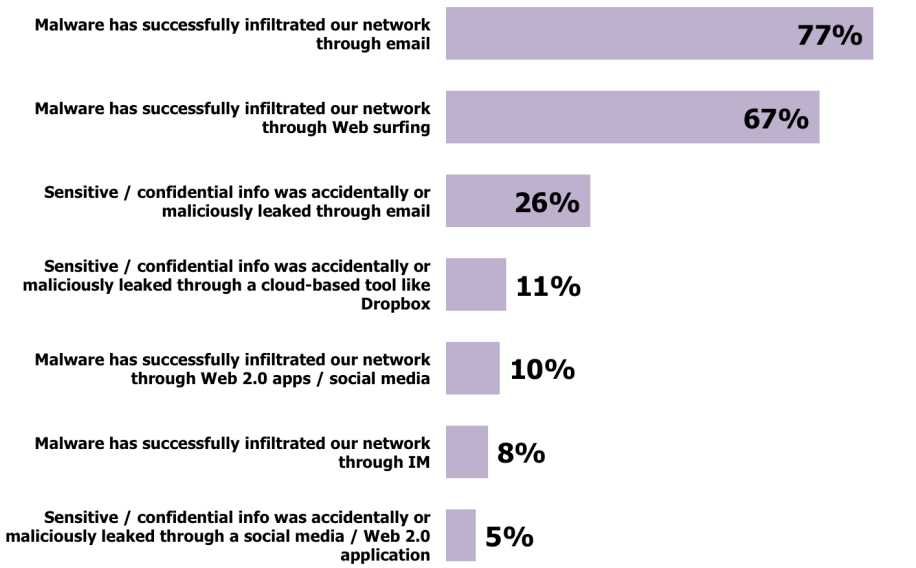
- **The ability to detect threats across all sources is essential**
  Email is the primary channel for the distribution of viruses, malware and advanced threats, but there are a number of other ingress and egress points for malicious content. For example, a leading security vendor has discovered a promoted Twittercard that can result in the installation of malware designed to steal Facebook credentials. Cybercriminals will often create bogus pages, such as a Facebook page, that will trick victims into downloading malware. Users are sometimes offered a desired capability, such as the ability to find out who visited their Facebook profile, and are willing to provide their login credentials or click on a link to obtain these "features".

  Consequently, protection from malware requires secure web gateways in conjunction with email gateways and file sandbox solutions. The benefits of an integrated approach are several, including the ability to correlate behaviors from different threat sources so that attacks and advanced persistent threats can be more easily identified, the ability to have threats detected in one system immediately propagate to other systems, easier and more consistent administration because policies and system management can be accomplished through a single pane of glass, and lower overall cost of security deployment and management.

  In short, security should enable use of multiple layers of threat protection, and policy management should be consistent and centrally managed across Exchange Online, the various Office 365 applications, and all other solutions. It is essential, therefore, to integrate secure web gateways and email gateway solutions to provide more complete protection for all of an organization's data assets.

- **Focus heavily on key threat vectors**
  A mature security capability must also focus heavily on all of the key threat vectors that organizations face, including phishing, spearphishing, malware, advanced persistent threats and other potential infiltrations or exfiltrations. Underscoring the importance of focusing on a wide range of threat vectors is the data in Figure 2, taken from a survey conducted by Osterman Research in November and December 2015, illustrating how common various types of threats have become.

Figure 2
"Which of the following has occurred in your organization during the past 12 months?"



Source: Osterman Research, Inc.

- **Identification of threats**
  Rapid identification of threats is also essential in order to minimize the Mean Time to Identify (MTTI, or "dwell" time) of zero-day and other unknown threats. Reducing dwell time to the greatest extent possible is vital, since the gap between infiltration of a network and its discovery permits cyber criminals to snoop around networks, discover valuable assets, and exfiltrate this content undetected. A 2015 Mandiant report found in situations where it had responded to a targeted attack during the previous 12 months, the mean dwell time was 146 days[xiii].

  A key element in the rapid identification of threats is the ability to correlate threats to threat sources, as well as the ability to scale this capability through the integration of data from billions of transactions each day. Cloud-based analytics is essential to perform this correlation, but there is variability between the cloud analytics capabilities offered by various security providers, and so vendors must be chosen based on their track record of being able to match threats and threat sources.

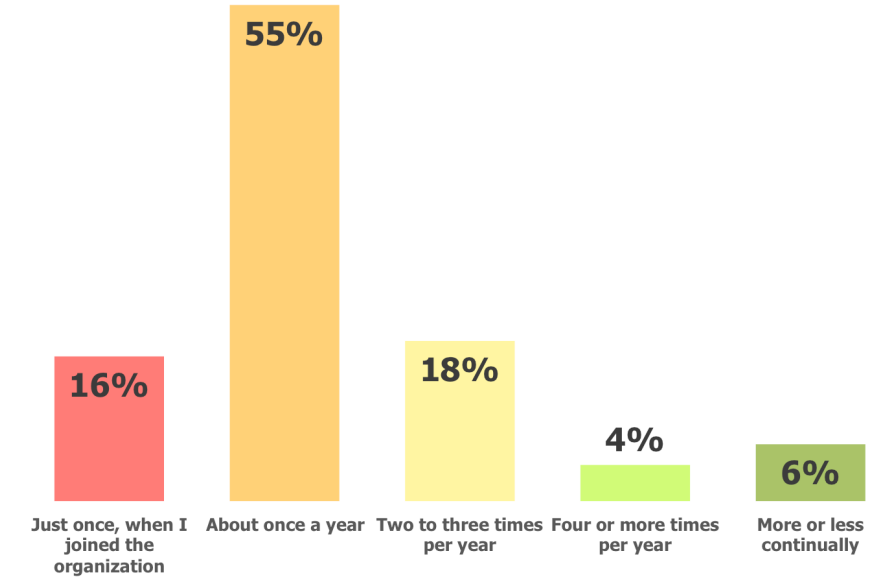
- **Sandboxing is essential to mitigate risks**
  The ability to sandbox threats is essential to mitigate risks. While sandboxing is not a foolproof method for detecting malware and other threats, it is a useful tool to detect and address various types of malware before they have an opportunity to infect endpoints or exfiltrate data.

However, not all sandboxing capabilities offer the same level of protection. Decision makers must pay attention to the comprehensiveness of the analytics they contain, which normally correlates with their maturity. Enterprise security companies have invested heavily into broad capabilities for discovering malware in files, including the ability of not alerting the file that it is being inspected. Good file sandboxes are complex and the result of years of evolution and investment. Microsoft's sandboxing technology has only recently been introduced.

- **Phishing education is an essential element in security**
  Finally, educating users about phishing and security best practices through a regular and well-planned program of security awareness training is essential to mitigate security risks. Users have always been the first line of defense in any security system, since a user not clicking on a link in a phishing email, not opening a suspicious attachment, or not visiting a dangerous web site is an effective tool for blocking various types of threats. While organizations must maintain robust security defenses on servers, gateway, in the cloud, etc., users remain a vital element in an overall security posture.

  It is important to note that users are perhaps more important now as a security defense than they have ever been, since the increasing efficacy of email, web and other security solutions means that cyber criminals are increasingly turning their attention to users as the "weak link" in the security chain. Some traditional security awareness training solutions are largely ineffective because they lack proper reporting and integration with email security solutions. Underscoring the extent to which security training is lacking in many organizations is the data in Figure 3 that shows just how infrequent security awareness training occurs.

Figure 3
"How frequently do you receive formal security awareness training?"



Source: Osterman Research, Inc.

RECOMMENDATIONS

Osterman Research offers four recommendations for organizations that are considering the deployment of Exchange Online:

- **Seriously consider Microsoft's offerings**
  Exchange Online represents Microsoft's 15-year-plus history of remotely hosted offerings that began in the late 1990s with hosted delivery of Exchange Server through a variety of business partners. Microsoft offers in Office 365 a robust set of offerings that include email, calendaring, scheduling, task management, desktop productivity, telephony, real-time communications, and collaboration services, most of which we have not discussed in this paper because our focus has been on Exchange Online. Plus, Exchange Online is offered in a variety of packages that allow decision makers to tailor these capabilities to their specific requirements, as well as those of particular groups within their organizations.

- **Understand their limitations**
  That said, there are limitations within Exchange Online – particularly with regard to its security capabilities – that may pose a problem for many decision makers, especially those in enterprises. Microsoft is good at a variety of capabilities, but its forte is not security. Leading enterprise security software vendors offer better security capabilities and should be considered as supplements and/or replacements for the native Exchange Online security capabilities, features and functions.

- **Consider the use of third-party solutions**
  Decision makers should consider the use of a third-party security solution that provides more robust and mature capabilities, particularly in the realm of DLP, file and URL sandboxing, threat identification and integrated email and web solutions that can protect against sophisticated, multi-stage attacks.

- **Invest for the future**
  Focus on Exchange Online as the primary element within Office 365 to secure, but take a longer-term view to security by focusing on solutions that offer mature security capabilities across the entire range of Office 365 applications that might be implemented.

SUMMARY

Exchange Online and Office 365 are robust offerings that include useful features and functions. The use of these platforms can drive down the cost of providing email and collaboration capabilities, and all organizations – including enterprises – should seriously consider their deployment. However, there are gaps in the security capabilities of the native Exchange Online offerings, and so any organization, but particularly enterprises, should seriously consider the use of third party solutions that offer more robust and mature security capabilities.

ABOUT FORCEPOINT

Forcepoint™ was created to empower organizations to drive their business forward by safely embracing transformative technologies – cloud, mobility, Internet of Things (IoT), and others – through a unified, cloud-centric platform that safeguards users, networks and data while eliminating the inefficiencies involved in managing a collection of point security products.

Forcepoint was established by uniting the user protection, data security and cloud expertise of Websense with the defense-grade insider threat and analytics technology of Raytheon and the next-generation network protection capabilities of Stonesoft. Unlike other security companies, Forcepoint have:

- Years of experience and the financial commitment necessary to build and deliver sophisticated, integrated systems.

- The ongoing ability to commercialize a unique set of expertise gained on the harshest cyber frontlines.

- A passion to relentlessly pursue solutions that empower our customers to move their business forward with cloud, mobility and other disruptive advances while simplifying their security environment.

That's why more than 20,000 organizations around the world rely on Forcepoint to reduce risk and handle threats so they can focus their full attention on what matters most to them.

Forcepoint's platform protects against threats from insider threats (accidental and malicious) as well as outside attackers, rapidly detect breaches, minimize "dwell time" – the period between compromise and remediation – and stop theft. With Forcepoint, organizations can protect users, networks and data in the cloud, on the road, and in the office. We simplify compliance, enable better decision-making and streamline security so that our customers can concentrate on what's important to them.
Our approach is to provide a unified cloud-centric platform to defend against attacks, detect suspicious activity sooner, and give the context needed to decide what actions to take to defeat the attack and stop data theft. Defend, detect, decide, defeat – this is our vision for Forcepoint 4D Security.

FORCEPOINT SECURITY FOR OFFICE 365

Our TRITON® 4D Platform powers a suite of products for web, email and data security that work together to protect your critical information as different parts of your organization begin to take advantage of Office 365. With Forcepoint, you can keep advanced attacks out and sensitive data in, across Exchange Online, SharePoint Online, OneDrive, and other Office 365 applications like Skype for Business. And because Forcepoint's unique approach keeps security close to your data – in the Cloud, on the road, or in the office – you can mix and match cloud and on-premise data security as you need it.

BEST INBOUND AND OUTBOUND PROTECTION, TOGETHER

Forcepoint complements Office 365 with an unmatched combination of protection against outside advanced attacks and insider data loss prevention (DLP) in a single solution, without complicated add-ons or "integrations". We guard your Exchange Online email against viruses, phishing, spam, Zero-Day Attacks, malicious code buried deep inside attachments, embedded URLs that point to disreputable websites, and much more – all powered by our global ThreatSeeker Intelligence Cloud which analyzes over 5 billion security events per day in over 155 countries.

In addition to keeping attackers out, Forcepoint keeps your critical data in. Our industry-leading DLP technology uses sophisticated means such as data fingerprinting, machine learning, optical character recognition, "low and slow" drip theft detection, and contextual analysis to detect and block attempts to move sensitive data to places it isn't supposed to go.

UNIFIED SECURITY ACROSS OFFICE 365 APPS – AND BEYOND

When migrating to Office 365, many organizations start with Exchange Online and then add other apps over time. Forcepoint makes it easy to immediately enforce the same level of data security in OneDrive, SharePoint Online, and Skype for Business, even Yammer, whenever you need it. As your use of Office 365 grows, Forcepoint keeps your data safe consistently, without having to recreate policies each time, learn new consoles, or juggle different reporting systems.

SECURITY IN THE CLOUD, ON THE ROAD, IN THE OFFICE

You should not have to choose between taking advantage of the Cloud and having the security, compliance and operations that various parts of your organization depend upon. Forcepoint uses a unique approach that puts security close to your data, wherever it is – in cloud apps, on roaming laptops or in your office network.

This makes it possible for you to use on-premise servers, endpoint systems, Office 365 services, and other cloud apps together – safely and efficiently. In an increasingly distributed world, we deliver holistic protection from a single console, with a centralized set of policies, and a single place to monitor and manage incidents in even the most sophisticated cloud-first and hybrid IT environments.

REFERENCES

[i] https://technet.microsoft.com/en-us/library/office-365-plan-options.aspx
[ii] https://products.office.com/en-us/exchange/compare-microsoft-exchange-online-plans
[iii] https://products.office.com/en-us/business/compare-office-365-for-business-plans
[iv] https://products.office.com/en-us/exchange/microsoft-exchange-online-protection-email-filter-and-anti-spam-protection-email-security-email-spam
[v] https://products.office.com/en-us/exchange/online-email-threat-protection
[vi] https://products.office.com/en-us/business/compare-more-office-365-for-business-plans
[vii] https://technet.microsoft.com/en-us/library/jj585024.aspx
[viii] http://www.fool.com/investing/general/2015/10/27/5-things-microsoft-corporations-management-wants-y.aspx
[ix] https://blogs.office.com/2013/10/28/office-365-compliance-controls-data-loss-prevention/
[x] http://www.msexchange.org/articles-tutorials/office-365/exchange-online/exchange-online-protection-quarantine-part1.html
[xi] $2.00 per user per month for Exchange Online customers ($1.75 for Exchange Online government customers)
[xii] http://www.msexchange.org/articles-tutorials/office-365/exchange-online/implementing-exchange-online-advanced-threat-protection-part1.html
[xiii] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/Infographic-mtrends2016.pdf