Osterman Research

WHITE PAPER

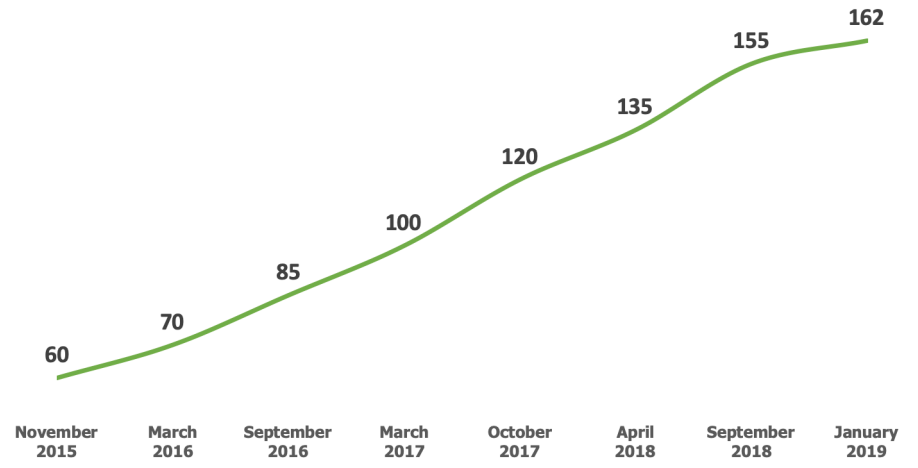
White Paper by Osterman Research
Published **June 2019**
Sponsored by **Mimecast**

Ten Questions to Ask About Your Office 365 Deployment

Executive Summary

By any measure, Office 365 is a success as millions of Microsoft seats transition from on-premises Exchange to a cloud-based email service as part of Office 365. While Microsoft has been offering hosted email solutions for more than 20 years, they have hit their stride with Office 365, the third major iteration of the company's foray into hosted/cloud-based email and collaboration. As shown in Figure 1, Office 365's growth has been significant over the past three-plus years.

Figure 1
Office 365 Subscribers Installed Base
Millions of Users



Source: Osterman Research, Inc.

Microsoft has included a wide range of applications and features in the Office 365 platform in addition to email, such as various security, archiving, collaboration, communication, encryption, authentication and other services. However, the primary communications and collaboration tool for most users – and the core of Office 365's functionality – continues to be email. By any measure email is a challenging application – arguably the most challenging – to deploy, manage and secure.

While Office 365 includes needed functionality to support the core email and collaboration capabilities of the platform, it will not meet all users' and all organizations' needs. Osterman Research's in-depth analysis of the Office 365 platform indicates that there are limitations with these services that should be considered by decision makers who are either considering a migration to Office 365 or have already deployed it.

There are limitations… that should be considered by decision makers who are either considering a migration to Office 365 or have already deployed it.

ABOUT THIS WHITE PAPER

This white paper discusses the key issues that decision makers need to consider as they evaluate the email, security, and resilience capabilities of Office 365. It was sponsored by Mimecast, information about which is included at the end of the paper.

Key Issues to Consider About Securing Email

Providing robust email security is a critical best practice for any organization in an era of increasingly sophisticated email-borne attacks, such as account takeovers, phishing, spearphishing, Business Email Compromise, ransomware, malware and

other threats. Phishing, in particular, has been identified as one of the issues about which decision makers are most concerned.

While Office 365 provides some native protections against phishing and other threats, there are some important limitations to consider:

- Mimecast has discovered a 16 percent false negative rate in spam and phishing detection within Office 365's native security over testing which included more than 100 million emails.

- Spoofed, lookalike and soundalike domains are a serious issue. Office 365 can notify potential victims of a suspicious message that spoofs the organization's domain name, but that match must be exact – the native capabilities in lower-level Office 365 plans won't deal with near matches because of similar domains that look or sound like the organization's domain. Higher end Office 365 plans are necessary, in this case the ATP Anti-Phishing Policy that comes with Office 365 E5 (or as an add-on for lower level plans). And, Office 365 also doesn't address domains that are similar to an organization's business partners or well-known Internet brands.

- Office 365's Safe Attachments capability uses virtual sandboxing to determine if there is malware or other potentially malicious attachments within an email. However, it's not effective against some of the more sophisticated threats, such as password-protected ransomware that is sent with the password in the body of the email. Many third-party solutions go beyond sandboxing on virtual machines to include the next-generation of detection mechanisms, such as recursive analysis of embedded documents, deep content inspection, static file analysis, evaluation of threats below the application and operating system levels, or sandboxing on controlled physical machines to analyze for malware that can evade virtual sandboxing detonation.

- While scanning for potential URL-based threats is key, the use of static blacklists is not an effective method of protection, since the system "learns" only when users somewhere have clicked on a link, become infected, and reported it – in effect, allowing some users to become victimized so that the majority of users can be protected. Because many phishing sites have very short lifetimes – often as short as a few hours – the use of dynamic site analysis is much more effective than the use of static lists.

Because many phishing sites have very short lifetimes – often as short as a few hours – the use of dynamic site analysis is much more effective than the use of static lists.

HYBRID ENVIRONMENTS

Many organizations will continue to operate hybrid environments of several different types, using combinations of both cloud-based and on-premises email management systems. Particularly for larger organizations, it is very unlikely that only cloud-based solutions will be used across the entire organization. Even if the goal is a 100 percent transition to the cloud, this transition can often take a long time. Dell, for example, believes that over the next several years, 40 percent of public cloud workloads will migrate to private cloud environments using on-premises infrastructure, resulting in an even greater proportion of organizations that will opt for hybrid email management deployments.

As a result, the ability to secure multi-platform, multi-vendor email environments is often essential. Because the Office 365 Advanced Threat Protection (ATP) offering does not fully support hybrid capabilities, customers with Exchange on-premises must deploy a second, separate threat-protection solution to compensate for these limitations[i]. For example, ATP Safe Attachments includes the Dynamic Delivery option that will eliminate email delays by sending through the body of an email message immediately, but will include only a placeholder for any attachments until they have been scanned by ATP Safe Attachments. However, Dynamic Delivery works only if the organization's email is hosted in Office 365 – if, for example, email is hosted in Exchange Server, Dynamic Delivery will not work[ii].

Of course, this adds increased system and administrative costs. Moreover, ATP won't address security needs beyond Office 365, which is a problem for organizations that operate non-Microsoft applications like Salesforce.

Continuity is a Best Practice

Office 365 is generally a reliable offering and normally does not suffer many global, long-term outages, although it does suffer shorter, more frequent and localized ones. For example, between February 6 and April 30, 2019, Office 365 suffered 18 separate outages totaling nearly 353 minutes in duration[iii] – that translates to an outage every 4.6 days. Moreover, while Office 365's overall uptime is quite good on a worldwide basis, it was slightly lower during the first quarter of 2019 compared to any quarter since the second quarter of 2017[iv].

The causes for the outages vary, but are sometimes a result of Office 365's dependence on Azure AD or DNS configuration problems[v], creating additional potential for outages in addition to problems that might occur with the Office 365 infrastructure itself.

Even short outages can have serious consequences. For example, users who cannot send email using their corporate Office 365 account will often revert to their personal email account to conduct business, thereby bypassing corporate security and increasing the likelihood that dangerous content – such as phishing attempts that contain malicious links or attachments – will reach end users. In addition, business records in email will not be captured by the enterprise archiving or backup systems. Overall business risk will increase because security, archiving and backup systems will be bypassed.

The key issue here is the lack of a redundant architecture in Office 365: there is no backup system to route email during outages. The use of a secondary, backup solution that will maintain the continuity of email processing is an important addition that will help organizations remain both secure and compliant during an Office 365 outage.

The key issue here is the lack of a redundant architecture in Office 365: there is no backup system to route email during outages.

Third-Party Backup and Recovery is Important

BACKUP IN OFFICE 365 OPERATES UNDER A DIFFERENT PARADIGM

Unlike conventional, on-premises email and other productivity solutions that are backed up on a regular basis, Office 365 operates under a different backup paradigm. It is important that organizations understand this. The platform does not include traditional backup and recovery capabilities in the same way as organizations have historically deployed them in on-premises environments. Office 365 is a live production system that offers recovery of messages and documents in a rolling time window only, and Microsoft uses a different approach for safeguarding current production data. For example:

- Data sent to the Recycling Bin from OneDrive can be recovered for 90 days, but only the most recent version of that data.
- In Exchange Online, users can recover deleted items for up to 14 days, but an administrator can increase the recovery window to 30 days[vi].

Another option that some organizations attempt to use to address the backup challenge is to use an indefinite legal or a selective litigation hold to prevent mailbox items from being deleted. The data will be hidden from the user's view when deleted,

but will still exist within the mailbox. In SharePoint Online, there is also the ability to retrieve a deleted file within 30 days of its deletion.

Microsoft does not offer point-in-time backup and recovery for organizations that want more traditional backup capabilities. Plus, it can't retrieve items that were deleted beyond their recovery timeframe (assuming the mailbox is not on litigation or legal hold.) Other disaster-level scenarios also are not covered by Microsoft's service offering.

Moreover, there are other risks of losing data in Office 365 because of a malicious attack, such as ransomware; careless or malicious users deleting content; and technical failures that could result in data loss. The reality is that once it is gone, there is a good chance it really is gone.

Other Issues to Consider

ROBUST SEARCH IS ESSENTIAL

Microsoft offers an email search capability within its eDiscovery toolkit in the Security & Compliance Center, but the use of these search capabilities requires that an eDiscovery case is created first. Once a case is created, one or more content searches can be created and saved within the case. Microsoft separately offers a Content Search option in the Security & Compliance Center. While Content Search is described as an eDiscovery tool, as well, there is no ability to create an eDiscovery case.

There are some limitations in Office 365's native search capabilities, such as an inability to search email attachments that are password-protected[vii], the inability to search documents that contain special characters, and the lack of optical character recognition[viii]. Some third-party archiving solutions address these limitations.

A SINGLE INTERFACE FOR SECURITY IMPROVES EFFICIENCY

The Microsoft Security & Compliance Center offers various threat reports, but these provide only a piecemeal view of the threats that face an organization across various threat vectors – it does not offer a consolidated view. These reports are focused on specific types of attacks, which means that a security administrator must manually correlate the issues that are occurring across the organization so that they can gain a "big picture" view. A better practice is to provide an open API and specific integrations with SIEM, SOARs, threat management, and other preventive security systems so that email specific threat information can be analyzed and used as part of an organization's entire security environment.

Having a security feature is not the same thing as having high security efficacy.

The Ten Questions You Should Ask About Your Office 365 Deployment

For any decision-maker considering an existing or future deployment of Office 365, Osterman Research believes that there are ten questions that should be asked – and answered to the satisfaction of all stakeholders.

1. **Why should you consider using a third-party solution since everything is included in Office 365?**
   It's true that Microsoft has included a wide range of capabilities within the various Office 365 plans, ranging from the more basic Enterprise Plan E1 (and lower plans) to the full-featured Enterprise E5. Office 365 includes a number of capabilities around security, archiving, encryption, authentication, etc. While Microsoft has clearly "checked all the boxes" in terms of providing these capabilities, there are some deficiencies in them relative to third-party solutions. Osterman Research has conducted extensive analysis on these features and

functions and determined that while they work as advertised, they are not necessarily best-in-breed and will not fully meet many organizations' requirements. Having a security feature is not the same thing as having high security efficacy.

2. **Is the "full meal deal" offered in Office 365 Enterprise Plan E5 adequate to meet all security, archiving, encryption and other requirements?**
To its credit, Microsoft offers a number of useful and important capabilities in its top-level SKU, Enterprise Plan E5. While this version of Office 365 includes a number of useful capabilities, not all of the capabilities will meet every organization's requirements. As just one example, some third-party anti-phishing solutions offer a better detection and capture rate than the native capabilities in Office 365.

3. **Can the cost of Office 365 be reduced by deploying lower level plans in conjunction with third-party solutions?**
As a corollary to the point above, the cost of Office 365 can be reduced by using a lower level plan along with various third-party solutions. For example, using Plan E3 instead of Plan E5 will save an organization US$15.00 per user in the United States and £13.20 in the United Kingdom. Given the current cost of competing security, archiving, encryption and various other solutions, organizations can put together a combination of Plan E3 (or, in some cases, lower plans) and third-party solutions to achieve a lower total cost of ownership than going solely with Plan E5.

4. **What would be the impact of data leaks or breaches resulting from email-borne threats such as phishing?**
The impact of even a minor data breach can be significant. For example:

    - A data breach can trigger various types of regulatory violations and requirements, including those of the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), Gramm-Leach-Bliley, the Financial Industry Regulatory Authority (FINRA), the Health and Human Services Office of Civil Rights, the Financial Conduct Authority (FCA) and any of the 50 US state data breach notification laws, among many others. These include reporting requirements (such as notifying victims of the data breach), fines and various types of sanctions.

    - Loss of reputation for the organization that breached data, including loss of reputation for senior company executives who must defend or explain the problems that led to the breach.

    - Loss of revenue from customers who refuse to do business with a company that breached their data or that of their peers.

    - Staff members can get fired, particularly senior staff members like the company CIO, CISO and others.

    - Significant expenditures on new security solutions like firewalls, EDR solutions and cloud security gateways, all of which are often deployed hurriedly, and thus are often unbudgeted.

    - Potentially significant reductions in a company's value, particularly for public companies. One analysis found that in Years 1, 2 and 3 following a data breach, a breached company's stock price underperformed the NASDAQ by 3.7 percent, 11.4 percent and 15.6 percent, respectively[ix].

5. **Will the organization use only Microsoft solutions, or will other vendors' solutions also be used?**
It is a rare company, particularly one with several hundred or more employees,

The cost of Office 365 can be reduced by using a lower level plan along with various third-party solutions.

that uses only Microsoft solutions throughout. It's common for organizations to have a combination of Microsoft and other vendors' solutions, and so it is imperative that the security, archiving, encryption and other technologies will work in multi-vendor environments. As just one example, an organization that relies solely on the native archiving capabilities of Office 365 will be unable to adequately archive their content from Salesforce Chatter, Slack or text messaging applications in the same archive.

6. **Will a third-party security solution, acting as an additional layer to the included Office 365 security solution (EOP), improve overall efficacy against phishing, malicious URLs, malware infiltration and other threats?**
   The answer to that question is generally yes. While EOP provides a solid level of basic protection against spam and malware, it does have deficiencies. Many third-party solutions offer a better level of detection and capture for spam and malware, while also offering more sophisticated capabilities focused on phishing detection, URL protections and the like. This doesn't mean that EOP does not provide useful capabilities, but only that it should be supplemented with a more robust set of security capabilities.

7. **How much of a risk and productivity loss will be introduced by occasional Office 365 outages?**
   The level of risk associated with an outage can vary substantially. While a very short outage might not be a problem, a more protracted outage – even one lasting just minutes or hours – can introduce substantial risk. During an outage employees will often switch to a personal email accounts, their personal mobile phone, or a personal Dropbox account, for example, to continue doing work. This will bypass corporate security and archiving systems and create opportunities for malware infiltration and gaps in the archiving of business records.

8. **Is use of a single platform/infrastructure adequate to provide proper backup and recovery?**
   Not really. Best practice dictates that any backup be stored in a completely separate infrastructure from the primary data source. However, Office 365 uses the platform itself to provide data protection, a violation of the best practice "3-2-1 Rule". Using an external system to protect Office 365 content is a better best practice. Moreover, Microsoft admits that point-in-time restoration of individual mailbox items is not included in Exchange Online[x].

9. **Just how important is high performance search for users, administrators or other specialists?**
   Even smaller organizations can generate significant volumes of data. For example, saving just 40 emails and files per day per employee for seven years in an organization of 500 employees will create an archive of 35 million archived elements. High performance search is essential to be able to find content quickly for purposes of eDiscovery, litigation support, end-user self-service, etc. This is an area that Office 365 often falls short of customer requirements.

10. **Will the native archiving and eDiscovery in Office 365 address all of your requirements?**
    It might. But our research has found that several third-party solutions can offer better capabilities than the native tools within Office 365. For example, if an organization needs to archive business records in tools that are not supported in Office 365, a minimum of two archiving platforms will need to be supported, driving up costs and increasing the complexity of and time required for searches.

During an outage employees will often switch to a personal email accounts, their personal mobile phone, or a personal Dropbox account…to continue doing work.

Summary and Conclusions

Office 365 provides excellent applications and service that should be considered for deployment by just about any organization. However, like any platform, it cannot be all things to all customers. Consequently, decision makers should perform due diligence on Office 365 to determine what it does well, how its capabilities mesh with existing organizational needs, and how third-party solutions can be used to supplement or replace its native capabilities.

About Mimecast

Mimecast is a cybersecurity provider that helps thousands of organizations worldwide make email safer, restore trust and bolster cyber resilience. Mimecast's expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy. From email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, human error and technical failure. **www.mimecast.com**

REFERENCES

[i] Based on Osterman Research evaluations of Office 365.

[ii] https://docs.microsoft.com/en-us/office365/securitycompliance/dynamic-delivery-and-Previewing

[iii] https://istheservicedown.com/problems/office-365/history

[iv] https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/service-health-and-continuity

[v] https://www.theinquirer.net/inquirer/news/3075066/microsoft-azure-365-outage-dns-Blunder

[vi] https://docs.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-user-mailboxes/change-deleted-item-retention

[vii] https://docs.microsoft.com/en-us/office365/securitycompliance/partially-indexed-items-in-content-search

[viii] https://www.office365tips.org/office-365-ediscovery-search-limitations/

[ix] https://www.comparitech.com/blog/information-security/data-breach-share-price-2018/

[x] https://docs.microsoft.com/en-us/exchange/back-up-email