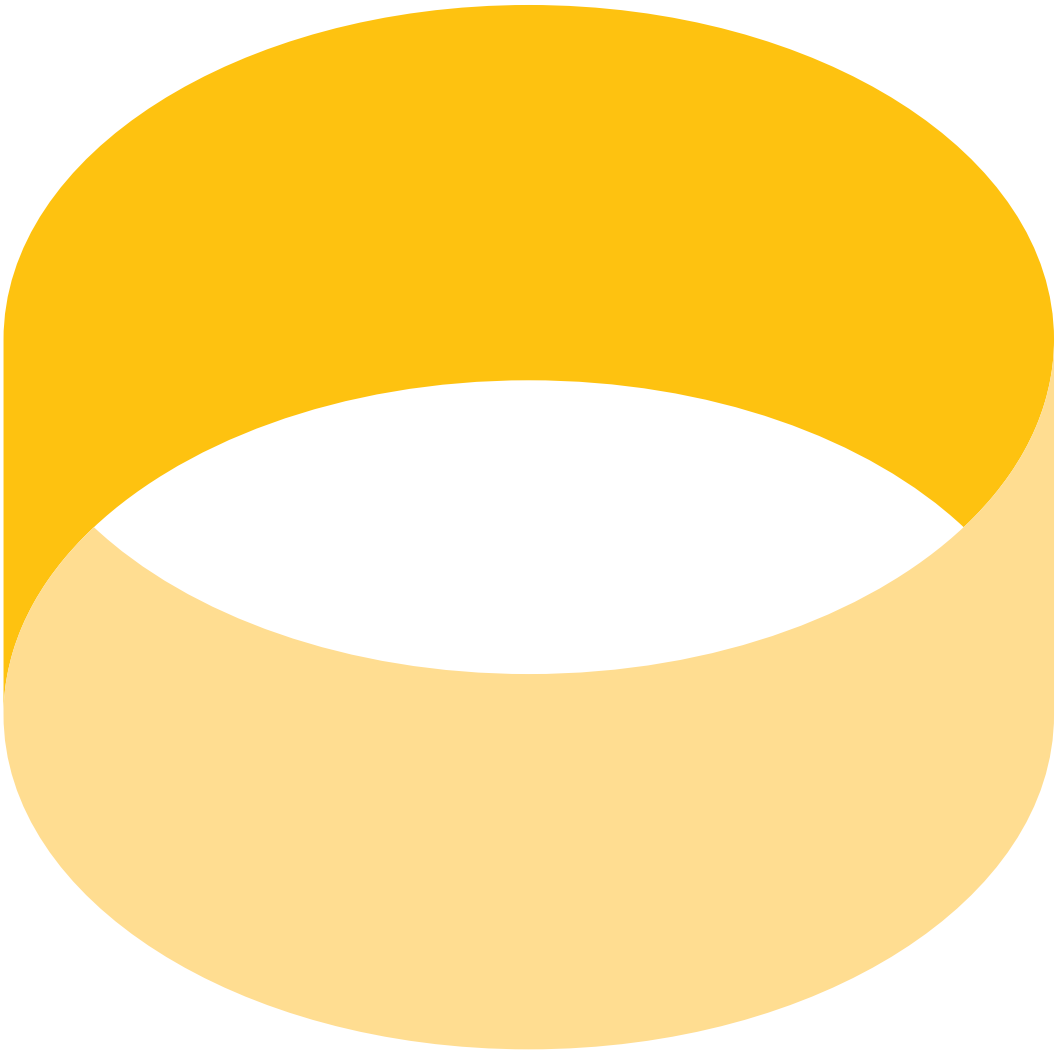

Start Your Implementation Planning for Office 365

WHITE PAPER

Author
Deena Thomchick
Senior Director of Cloud, Symantec

single point of contact

Symantec™

Ready, Set, ...Wait, What?

You know you are adopting Office 365. Whether you are just wading in with a partial Exchange Online deployment, jumping right into the deep end with a full-cloud, everything Office 365 adoption or something in-between—the decision is made and you are moving forward as fast as you can. Before you take off running with any SaaS adoption you should consider key decisions you will need to make when implementing Exchange Online and other aspects of Office 365. Take a moment to review how you will approach the following topics addressed in this paper; they could impact your Office 365 role out "to do" list.

Performance Planning

You'll likely reduce your Microsoft licensing costs with a move to O365 but you will increase your bandwidth requirements and the number of open internet connections in addition to introducing new security requirements. So, make sure to allocate budget to accommodate security requirements for O365. Too many companies have been blindsided by this requirement.

A typical Exchange Online user will require 6 or more open internet connections when operating the application and will generate a 200MB increase in internet traffic. Are you ready to accommodate this increase in internet traffic and number of simultaneous connections?

Have you evaluated your internet bandwidth and network infrastructure to see if you are ready for this increase?

Are your security solutions prepared to handle this increase in traffic? (Despite some tendencies to reduce security to accommodate O365 connections, this is a highly risky strategy considering today's threat landscape—the budget you save now may come back to cost you a lot more later.)

Security Readiness for Office 365

There are a number of security issues to address when you start planning the adoption of a cloud app, especially one as central to your business as Office 365. Are you prepared to add additional security to safeguard your organization and stay compliant when much of your business moves into the O365 cloud?

Elastica analyzes more than 85 individual characteristics across seven categories to evaluate the Business Readiness Rating for a cloud app. We used our analysis of Office 365 attributes and our experience with big cloud app adoption projects to compile the following planning categories for you to consider.

- Access Controls
- Service Characteristics
- Administrative Controls
- Compliance and Responsibility
- Data Protection and Governance

Access Controls for Office 365

What password controls, authentication and identity systems will you set up for your Office 365 implementation? Office 365 is one of the more business ready cloud platforms and it has a good range of access control options to navigate. Attackers target account credentials for theft so it is important to implement a secure user authentication and user access strategy.

What do you want to use for Federated Identity Management? Will you use OAuth or SAML? Office 365 doesn't support OpenID.

How would you like to protect your accounts against brute-force attacks? You can utilize CAPTCHA or set up progressive responses if there are multiple failed logins.

You should implement Multi-factor Authentication (MFA). Passwords alone are not secure enough, especially for a system as core to your business as Office 365. With Office 365 your MFA can be delivered via SMS or mobile app. Office 365 does not natively support MFA via USB Token, Smartcard, secondary email, Security Questions, or Biometrics at this time. If you want these options you'll need to look into a Single Sign On solution that provides these services.

Decide what your password quality requirements will be. Office 365 will require a minimum length and a strong format for your passwords. It will also force your users to change their password periodically. And if your users forget their password, there is a native provision for password reset and recovery.

Do you want to set access controls that restrict what devices can be used with Office 365? You can do that but you can't limit logins based on a range of IP addresses. Do you want to control what devices can do with Office 365? For example: BYOD devices can access Office 365, but files cannot be downloaded to unmanaged devices.

You'll probably want to take advantage of the integration available with Active Directory (AD). Most organizations use AD and hopefully you do because Office 365 does not offer LDAP integration.

Do you have a Single Sign On solution already in place that you will use for Office 365? If you don't, you may want to adopt one that can handle multiple cloud applications as well as internal or private cloud systems.

Office 365 Service Characteristics

Office 365 is hosted on a private Microsoft hosting platform. It is multi-tenant and customer data is separated at the data level.

It is available as a web based service and supports both a desktop client and a native mobile app. If you enable all of these methods for using Office 365, you should consider whether you need to set up some additional security controls depending on the method of use. You may want to require multi factor authentication (MFA) if a user comes into their accounts via a mobile app or the web interface.

Have you thought about connecting other apps or your website to Office 365? This is an option available to you. Office 365 has an API catalog in their Office Dev Center online and all their APIs are REST services.

Administrative Controls

What administrative access controls will you require? Will you take advantage of the role-based access controls available in Office 365? Do you already have defined roles or do you need to create them?

Audit trails are important for compliance and incident response. You will be able to track administrator and end-user activity with native Office 365 controls but this visibility will be limited to what happens in your Office 365 corporate accounts. You won't have audit trails for activity that goes beyond this boundary into your on-premises environment or into other cloud services unless you put a third-party cloud access security broker (CASB) in place.

What policy controls do you want to set up? Office 365 offers some options here but it does not natively include content classification for policy control and it is limited to the Office 365 environment as well as Microsoft platforms. If you want to set up content identification and classification, policy controls, and auditing that reaches beyond the Office 365 boundaries, you will need to look into additional cloud security options such as a CASB or cloud DLP solution.

Compliance and Responsibility

It is likely that you are planning to keep sensitive, compliance related data in Office 365. Microsoft meets most of the compliance requirements including: CSA STAR Self-Assessment, PCI, HIPAA, ISO 27001, SSAE 16 SOC2 Type II, ISO 27018, SOC I type 2, GAAP, FISMA, ISAE-3402, NIST SP 800-53, and FedRAMP. It does not offer Truste, Safe Harbor, SOC III, ITAR, or COBIT at this time.

Be sure to read the Office 365 publicly available Service Level Agreement to make sure you are very familiar with what security activities Microsoft is responsible for and what it is not responsible for with Office 365. In particularly it is important to note that Microsoft will not take responsibility for the data your users choose to upload and share in Office 365 and Microsoft do not take responsibility for unauthorized user access to your accounts if one of your employee's account credentials are compromised.

Data Protection

Office 365 provides some basic protections for your data. It encrypts data at rest in the Office 365 cloud. It does not encrypt your Office 365 data when it is stored outside the Office 365 cloud, whether offline on an endpoint or in another cloud.

Office 365 provides 2048 bit or greater SSL for protecting data in motion and it is secured against the OpenSSL, Heartbleed, Logjam, FREAK, CRIME, or DROWN vulnerabilities. That said, Office 365 does not support TLS_FALLBACK_SCSV which is a well known remedy against the POODLE attack. Nor does it support HTTP security headers such as HTTP STS, X-SXX, X-Content, and X-Frame.

There are sharing controls for both internal and external users available in Office 365. You will need to decide if you want to allow your users to share with external users or not. Collaboration platforms like Office 365 are very powerful business enablers but inadvertent over sharing is the biggest cause of sensitive data exposure for enterprises. So make this decision with the awareness that you should probably also create a plan for how you will educate your users on responsible data sharing practices. And, consider putting

data governance and cloud DLP controls in place to protect accidental data exposure. This is another reason Gartner highly recommends you adopt a CASB when you adopt platforms like Office 365. Can you extend your existing DLP solution (if you have one) to Office 365 with a CASB?

Threat Protection

Compromised user accounts present a real threat to your organization and with potentially thousands of user credentials in play, the prevalence of malware targeting user credentials and the ability to access Office 365 accounts directly from the internet, it is statistically likely you will have user accounts that get compromised. The best way to identify a compromised account is through user behavior analysis (UBA). Office 365 will analyze your data for with basic UBA but it may not provide the same level of UBA intelligence as other systems. It is limited to only Office 365 accounts and can't analyze user behavior across multiple cloud apps. It does not analyze your data for ad targeting.

Let the Planning Begin

Now that you have a sense of some of the security decisions you will need to make as you adopt Office 365, you are ready to start your deployment planning. Here is a sample plan you can use to document and track your progress:

Office 365 Adoption Security Plan

DATA GOVERNANCE AND PROTECTION

1. Develop a Data Classification Plan: Can you use your existing DLP solution? Can you use a CASB for this? A home grown classification system requires a lot of work to develop and maintain.

2. Detect risky data in Office 365: If you already have Office 365 in flight, find out where your current risks exist. Going forward, perform ongoing monitoring of sensitive data in Office 365 with a CASB.

3. Implement policies to prevent sharing of risky data: You can perform fast remediation through CASB API integration and you can prevent over sharing before they occur with CASB gateway controls.

4. Implement policies to limit capabilities of unmanaged devices, such as a policy preventing downloads to unmanaged devices.

5. Identify users who are sharing risky data and train them: targeted notifications can be very effective at correcting risky user behavior.

6. Encrypt data with compliance requirements: Identify if encryption capabilities within a CASB or natively in Office 365 will meet your requirements. They may not if you need to address strict requirements mandating that your enterprise maintain complete control over your encryption keys.

7. Process to generate monthly data risk report: Make sure you know what's going on and can report out to management on a regular basis to help you with planning and provisioning going forward.

COMPLIANCE AND DATA PRIVACY

8. Identify regulated data that is being placed in Office 365: The same DLP and/or CASB solution that identifies sensitive data should cover this with particular focus on key compliance-related classifications.

9. Identify legitimate business reason for regulated data present in Office 365: Is there data that can be restricted from Office 365, negating the requirement to secure that data in the cloud at all?

10. Restrict regulated data from O365 if there is no legitimate business reason: Create automated policy controls and security measures in place to prevent regulated data from being upload to Office 365 at all, if it isn't necessary to store it there. A gateway control can block this data from being uploaded to the cloud.

11. Implement policies to restrict regulated data from being shared in the cloud: Create automated policy controls. An API-based CASB can quickly remediate unsafe sharing, a gateway-based CASB that can read sharing transactions in-line in real-time traffic can prevent unsafe sharing (not all CASBs can do this).

PERFORMANCE AND SECURITY

12. Scope number of users and proposed adoption timeline: Decide how fast you want to roll out Office 365. Most enterprises take a hybrid approach for a while before going all in.

13. Identify average bandwidth and connections required per user: Blue Coat research has identified that the average user will need an additional 200 Mbps of bandwidth and 7 concurrent connections for a Microsoft Exchange deployment. Additional Office 365 applications will easily add an additional 100Mbps and can require 40+ concurrent connections.

14. Provision existing security systems to handle increased bandwidth and connection requirements: You will probably need to add resources here to accommodate additional internet traffic.

15. Tune gateways to optimize performance: Take advantage of Office 365 performance tuning and traffic shaping in your gateways and firewalls.

THREAT DETECTION

16. Implement Single Sign On and Multi Factor Authentication for all sanctioned cloud apps: Cloud apps are accessible directly from the internet so access controls are critical to your security.

17. Implement DLP: Extend the DLP you already have in place via a CASB integration or look at adding DLP capabilities. Take advantage of a solution that can provide data classification for you.

18. Analyze user behavior in cloud applications with CASB: Identify and mitigate compromised Office 365 accounts using user behavior analysis with cloud visibility and enforce protections with automated policy controls.

19. Implement email protection: Email is a primary attack vector for attacks, be sure you have effective email protection. Evaluate whether your current email protection can be extended to Exchange Online or if you need to add new protections. If you don't have email DLP, identify how to add it.

20. Implement ATP protections: Stop malware from compromising your accounts and infecting your organization. Anti-malware and advanced threat protection is a key security practice that should be extended to your cloud accounts.

Conclusion

Congratulations on your move to Office 365. You will gain many benefits from your move to a collaborative cloud solution. However, you have an array of decisions to make and actions to take to make sure your organization successfully and safely adopts Office 365.

Analyze and review your options for protecting your organization against risks specifically associated with this core business move to the cloud. Benefit from what other organizations have learned along their adoption path and include security in your Office 365 implementation planning process from day 1 (or as soon as possible thereafter). Be aware, you will need to add new cloud security defenses and you will need to adjust your current security defenses to make sure your organization is protected.

Symantec and Blue Coat offer industry leading DLP, data science-driven CASB, SWG, ATP, endpoint protection, and email security to assist enterprises adopting Office 365.