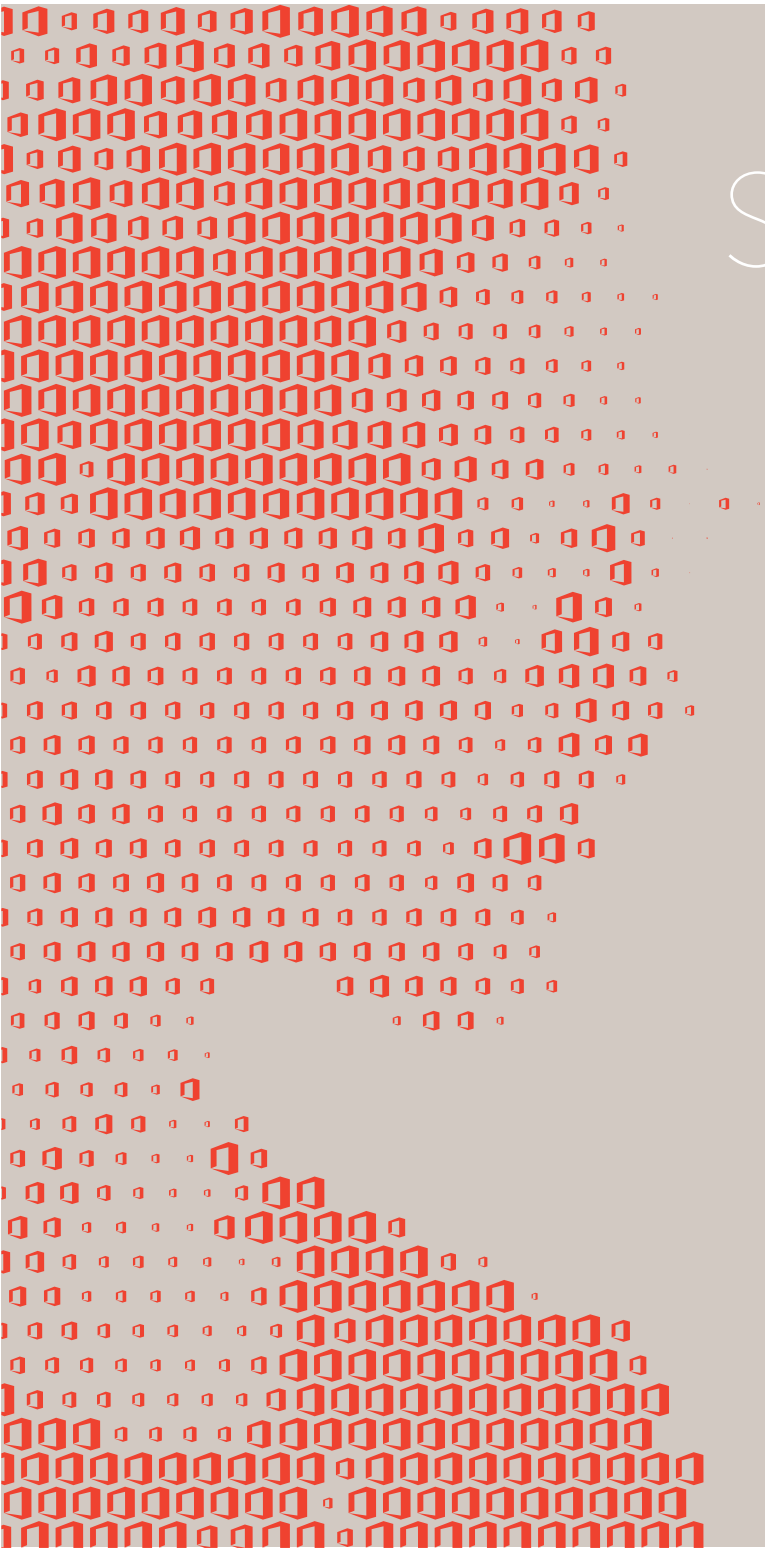
Symantec + BLUE COAT
Defining the Future of Cyber Security

WHITEPAPER



Safely Adopting Office 365

AN EXECUTIVE GUIDE

AUTHOR
Deena Thomchick
SENIOR DIRECTOR OF CLOUD, BLUE COAT

Symantec + BLUE COAT
Defining the Future of Cyber Security

Safely Adopting Office 365

AN EXECUTIVE GUIDE

Introduction

The writing is on the wall. Nearly every company will move to Office 365 sooner or later. Between the productivity and collaboration business advantages to the budget friendly opex licensing model to the fundamental reality of Microsoft's development focus on Office 365, it is only a matter of time. Already Office 365 is the #1 most deployed cloud application and 78% of enterprises currently use it or are planning to use it.

Most organizations start their Office 365 adoption with a move to Exchange Online for email and calendar—making Exchange Online the #1 selling O365 plan. Exchange Online is followed by OneDrive for file sharing in second place and ProPlus for a broad array of Microsoft applications in third place.

Key Considerations

Data sharing and data movement is key element of any O365 adoption—from an Exchange Online plan that comes with a 50GB mailbox, the Outlook app, and OneDrive to the full ProPlus packages. Starting with the very first step, a move into the world of Office 365 introduces a number of issues to consider.

1. Lots of enterprise data will now be stored in the Microsoft cloud, accessible by a wide array of users, and outside traditional enterprise IT control. This introduces privacy, security and compliance considerations.
2. Data will be transmitted back and forth between the cloud and endpoints—endpoints that may or may not be located within the enterprise perimeter and may or may not be managed by the enterprise. This introduces many avenues for getting in, out and around an organization's defenses that could be used by threats.
3. Your infrastructure will have many more concurrent open internet connections and higher volumes of data moving through your perimeter. So you will need to accommodate and manage more network traffic to maintain performance service levels.

Gartner identifies both security and performance as key issues to address when adopting O365. Many organizations don't consider either in their initial adoption plan and are left scrambling to find budget and insert implementation time for these items.

Who Is Responsible for Security in Office 365?

You are responsible for securing your users and content in your O365 accounts. Microsoft will provide infrastructure services to ensure hackers don't gain access to their servers and that their employees are vetted and can be trusted not to exploit your data. However, Microsoft doesn't take responsibility for controlling what, how, and with whom your employees and other users share data within your Office 365 accounts. In addition, they will not take responsibility for what content users upload into the cloud. In other words, they will not govern how your users use the service.

Accidental misuse, hacking, and malware typically come in through the front door of your O365 accounts which is likely why in 2016 Gartner predicted that, "95% of cloud security failures will be the customer's fault."

Adopting Office 365 will deliver any number of benefits to your organization but you must keep in mind that you will need to adjust your security provisioning in order to control sensitive content sharing in the cloud and to protect your organization against threats, hacks, and user errors that come along with O365 usage.

Start Planning and Budgeting Now

Too many organizations focus on planning and budgeting their roll out of Exchange Online or extended Office 365 plans without simultaneously provisioning for added security and performance requirements.

Cost and planning for Microsoft services

Are you just moving to Exchange Online or are you adopting a broader Office 365 approach? Which plan is the right plan for your organization? How fast are you switching users over? What is the scale of your adoption? Gartner research suggests that adoption may be slow and steady while many enterprises run both Exchange Online and traditional Exchange operations simultaneously for some time to come.

Plan and budget to add security

You will need cloud data governance, protection, DLP, access control, and threat protection. Perform a critical analysis of the in-house Microsoft security options and decide what is good enough and what isn't when it comes to securing your organization. Consider compliance requirements and perform a risk analysis for your organization. Try to be realistic about the manpower that may be required for some security systems. Gartner predicts, "By 2018, 40% of Office 365 deployments will rely on third-party tools to fill gaps in security and compliance..." (SOURCE: GARTNER, "HOW TO ENHANCE THE SECURITY OF OFFICE 365") It is possible that Gartner is being conservative with this prediction, adoption may be significantly higher for mid-to-large enterprise organizations.

- Plan for key third-party security additions such as a Cloud Access Security Broker (CASB) and advanced threat protection (ATP).
- Expand security coverage of your existing DLP and threat protection solutions to accommodate data in the cloud.

- Evaluate your access management, you may want to add or expand Single Sign On and multi-factor authentication.

Provision for performance

Evaluate the ability of your perimeter security and networking services to accommodate dramatic increases in data volume and number of concurrent internet connections—network routers & switches, web gateways, firewalls, IPS, and other perimeter protection and networking systems and services. For example: a typical user of Exchange Online will maintain 6 or more concurrent internet connections and an organization with 3500 people using Exchange Online likely will require an additional 200MB of internet bandwidth. Add additional O365 apps and concurrent connections can grow to 40+ and bandwidth increases to 300MB or more. This will likely require you to scale up so take advantage of capabilities in these systems to optimize traffic handling for better performance.

Safeguard Against Unauthorized User Activity

Microsoft will protect the backend of your O365 cloud but you must protect your O365 accounts as if they were one of your internal systems—because they are. You should focus on user access and activity and put protections in place to prevent unauthorized access and to identify and mitigate unauthorized activity in your accounts. Attacks, breaches and data theft require action and action is driven by users (or entities posing as users).

Secure access to O365 accounts

Put protections in place to prevent unauthorized access to your accounts.

Implement a single sign on solution (SSO) if you do not already have one. It is likely that O365 will not be your only system that requires secure access so look for a solution that can handle multiple applications—not just O365. If you already have SSO, this could be as easy as adding O365 to your existing solution. If you do not have an SSO solution in place, there are a number of SSO options available, including one from Symantec.

Add multi-factor authentication into your access requirements for O365. Passwords are not secure enough considering today's threat landscape. Hackers use brute force attacks to guess passwords and users commonly use the same or a variation on the same password for multiple accounts; so even if your systems stay secure, a data breach elsewhere can expose passwords that can be used to gain access into your accounts.

Identify and mitigate suspicious user activity

There are any number of ways your data and accounts can get exposed. Users with legitimate access can accidentally expose your accounts due to malware-driven session hijacking. You could be one of the unlucky organizations to have a malicious insider. However, most often, confidential information gets exposed through accidental misuse by users that simply make mistakes.

Put a good Cloud Access Security Broker (CASB) solution in place. Look for a CASB that includes a user behavior analysis system good at identifying abnormal and suspicious user behavior in the cloud and that also offers automated policy controls to mitigate damage that can result. You want something here that gives granular visibility into user activity and makes it easy to accurately identify and act on suspicious behavior.

Prevent Data Exposures

Set up a strategy to monitor and govern sensitive data in the Office 365 cloud

You will have confidential and compliance-related content in your O365 accounts. Considering miscellaneous errors and insider misuse are the #1 and #2 most common reasons for a security incident involving a data breach (SOURCE: VERIZON DATA BREACH INVESTIGATIONS REPORT, 2016), you will need a way to govern and protect your data in the cloud.

Cloud file sharing makes collaboration easy but it also makes over-sharing sensitive data easy as well. Twenty-three percent of files in the cloud are broadly shared and 12% of these files contain sensitive or compliance related data. (SOURCE: ELASTICA SHADOW DATA REPORT, 2016)

Broad sharing can lead to accidental exposure which typically involves inadvertent public sharing or sharing to very large groups of people. It can happen easily due to inherited file and folder sharing permissions or legacy sharing with individuals no longer affiliated with an organization.

Identify & classify sensitive content

The ability to effectively identify and classify data that is confidential or compliance related is key—especially when it is in the cloud where oversharing is so prevalent. This is a critical capability for a useful and effective DLP solution. Developing and maintaining a home grown identification and classification system is very time consuming. You will save a lot of manpower by leveraging a DLP solution that helps you classify your data.

Prevent & remediate oversharing of sensitive content in the cloud

Set automated policy controls to prevent your sensitive data from being exposed. This requires you to have visibility and control over all your data in the Office 365 cloud including the ability to:

- Monitor & control sensitive data moving to and from O365 using gateways and preventative endpoint controls
- Monitor & control data stored and/or created in the O365 cloud regardless of when, how, or from where that data was put into the cloud
- Monitor & control cloud-to-cloud sharing between O365 and other cloud apps

Add CASB for visibility and control

A good CASB will alert you when sensitive data is at risk in the cloud and will offer automated prevention and remediation in the event that confidential information is exposed. In addition to excellent visibility and policy controls, a good CASB can offer DLP based on dictionaries, data science-driven content analysis, and custom content learning systems. An even better one will integrate with your broader DLP solution if you have one. If you have decided to allow confidential data in the cloud, you can use CASB systems to automatically encrypt sensitive data in the cloud—adding additional protection against data breach.

Add Cloud DLP for extensive data identification, classification and protection

Identify and protect confidential data across your organization with a DLP solution that secures both your cloud accounts and on-premises systems. It is likely that you will have confidential data in a broad number of applications and a consistent, high-quality DLP solution will provide consistent protection as well as minimize the manpower associated with preventing data loss.

If you already have a DLP solution in place, you need to figure out how you are going to expand that protection to identify and classify all your data in the Office 365 cloud. There are a few CASB to on-premises DLP integration options available to choose from, however the only cloud to cloud integrated CASB + cloud DLP solution available today comes with a combination of Symantec DLP and Elastica CloudSOC.

Stay Compliant

Compliance related penalties have increased in recent years so staying compliant with regulatory requirements is more important than ever – especially for finance, healthcare, retail, and telecom. Most compliance regimes can be boiled down to two key requirements: you must perform a risk assessment and you must act responsibly to safeguard specific types of data.

Visibility is key to risk assessments

Look at the visibility options native to O365 as well as in a CASB solution. You will want the ability to look directly into your O365 accounts in addition to inspecting traffic in-line. Visibility directly into O365 makes sure you don't miss data in your O365 accounts uploaded through unmanaged remote devices, through direct cloud-to-cloud transfers, or created natively in 0365. You will also want visibility and control over in-line traffic where you can prevent risky actions and monitor user behavior at a very granular level – both associated with your 0365 apps and other cloud apps.

Protect compliance related data

Use data governance, encryption and DLP to prevent your organization from exposing PII, PHI, PCI, and other data governed by data privacy regulations. Some compliance regimes will require you to encrypt files and data that go to the cloud and some will require that your enterprise organization maintain control over your encryption keys (in these cases, you will not be able to use an encryption solution that requires Microsoft or your CASB provider to maintain your encryption keys in their cloud). Review PII, HIPAA, and GDPR rules to make sure your organization is ready to meet those standards.

Prevent Destruction & Theft

You must put protections in place to safeguard against attacks in your 0365 accounts—whether these attacks are malware looking for a method to infiltrate your organization, ransomware or bad actors bent on data destruction, attacks looking for a way to exfiltrate data from within your organizational perimeter, or threats hunting for valuable data to steal. It is critical that you have defenses in place to protect your organization against compromised accounts. Companies have thousands of credentials in use by their employees that grant access to valuable data, a compromised of any one of these credentials can open the door to significant damage.

Identify malicious activity

There are a number of technologies that can help you automatically identify threats in your cloud accounts—from identifying known malware, identifying malicious activity, and teasing threats into exposing themselves. Look at how you can apply a layered approach using all of the above to reduce the risk to your organization.

Identify and control compromised accounts

Implementing a CASB or other solution with strong user behavior analysis (UBA) capabilities is an excellent way to identify and mitigate damage caused by compromised Office 365 accounts. This method can identify threats difficult or impossible to identify through other threat protection methods.

Automate anti-malware for your cloud

Add anti-malware solutions that scan and remediate malware infections in your cloud accounts. These are an efficient and easily automated layer of protection. While you are at it, protect as many of your endpoints as you can—an infected endpoint is a great way for threats to get into your cloud.

Add advanced threat protection

Look at putting a layer of advanced threat protection in place to analyze files moving in and out of your cloud accounts (including but not limited to 0365). These remedies are available as cloud services and/or on-premises solutions and they take advantage of sandboxing and code emulation to tease previously unidentified malware into exposing itself. This is a valuable layer of protection in today's polymorphic and highly targeted world of malware.

Be Prepared

You will eventually have a security incident. When that happens, you want to be able to respond fast to remediate damage and prevent future incidents.

The key to incident response lies in the ability to identify an area of concern and then to find the relevant data in enough usable detail to parse out what happened. You need a system that can quickly identify if there is an area of concern that requires investigation. You need to easily find just the information that relates to the issue you are investigating. Then you want useful information in enough detail to perform an effective

analysis. And, finally, you may want to analyze data from multiple sources with a Security Information Event Management (SIEM) solution.

Getting the right level of visibility and log data for activity in cloud accounts can be difficult. Look for CASB, ATP, SWG, and other security solutions that provide high quality logs and are able to easily integrate with your central analysis systems.

Take a Wide Angle View

Today you may be specifically looking at adopting 0365 but this is likely not the only cloud application your organization will use. You are probably already using any number of other business enabling cloud solutions. When you look at implementing security for 0365 or any other cloud application, be sure to weigh both the benefits of a consolidated third-party security solutions and the native security provided by individual cloud app providers. No cloud app is an island. Each cloud you use is part of the integrated whole of your organization's infrastructure and collection of intellectual property. Gartner predicts that 40% of organizations will choose to secure 0365 with third party security solutions. A third party cloud-agnostic solution may provide broader visibility, consistent security capabilities, and generally higher effectiveness across multiple cloud apps that is more manageable by your IT organization.

In Summary

Congratulations on moving forward with your 0365 adoption. You will realize a number of business benefits with this move. However, to safely and effectively adopt 0365, you must also budget and plan for additional security measures and you will probably need to provision up to accommodate higher internet traffic volumes.

Safely adopting 0365 requires you to address the following requirements:

- Secure access to your 0365 accounts with SSO and MFA
- Safeguard against suspicious user behavior in 0365 accounts with user behavior analysis and CASB
- Protect your sensitive data in the cloud against loss with CASB and DLP
- Architect your 0365 implementation for regulatory compliance with risk analysis and excellent cloud visibility and security controls
- Safeguard against malware and advanced threats in your 0365 cloud with UBA, anti-malware, and ATP
- Prepare for effective incident response if/when you have a security issue with excellent logging and reporting from all your security solutions
- Provision your organizational infrastructure for an increase in internet traffic and connections, you may need to scale up or performance optimize all your network and security solutions that handle internet traffic

About the Author

Deena Thomchick is Senior Director of Cloud at Blue Coat. She's spent more than 25 years in technology with a particular focus on security. Her background includes work on encryption, advanced threat protection, network security and endpoint security.

About Blue Coat & Elastica Cloud Security

Blue Coat, Inc. is a leading provider of advanced web security solutions for global enterprises and governments, protecting 15,000 organizations including over 70 percent of the Fortune Global 500. Through the Blue Coat Security Platform, Blue Coat unites network, security and cloud, protecting enterprises and their users from cyber threats—whether they are on the network, on the web, in the cloud or mobile. Blue Coat was acquired by Bain Capital in May 2015. On June 12, 2016, Symantec and Blue Coat, Inc. announced they have entered into a definitive agreement under which Symantec will acquire Blue Coat for approximately $4.65 billion in cash. The transaction has been approved by the Boards of Directors of both companies and is expected to close in the third calendar quarter of 2016.

Elastica, acquired by Blue Coat in November, 2015, is the leader in Data Science Powered™ Cloud Access Security. Its CloudSOC™ platform empowers companies to confidently leverage cloud applications and services while staying safe, secure and compliant. A range of Elastica Security Apps deployed on the extensible CloudSOC platform deliver the full life cycle of cloud application security, including auditing of shadow IT, real-time detection of intrusions and threats, protection against intrusions and compliance violations, and investigation of historical account activity for post-incident analysis.

For additional information, please visit elastica.net.