International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 5 Issue 6, June-2016

Experimental Analysis for Microsoft Office 365 enhanced with Cloud Computing

Syed Jibran[1], Dr. Yashpal Singh[2]

[1]Research Scholar, Computer Science & Engineering Dept., GITAM, Kablana, Jhajjar, Haryana
[2]Associate Professor, Computer Science & Engineering Dept., GITAM, Kablana, Jhajjar, Haryana

ABSTRACT

Microsoft Office 365 represents the company's latest entry into the cloud-based messaging, collaboration and productivity market. While deciding on which of the many flavors of Office 365 to deploy can be a bit daunting because of the many (and somewhat confusing) options available, it is clear that Microsoft has done quite a good job at creating a robust and scalable platform that can satisfy the requirements of many organizations.. Along with the encryption technologies in Office 365 that are managed by Microsoft, Office 365 also includes encryption features that customers can manage and configure. This greatly enhances the security and agility of the service. We regularly conduct penetration tests to enable continuous improvement of incident response procedures. These internal tests help our security experts create a methodical, repeatable, and optimized stepwise response process and automation.

Keywords: Microsoft, office, security, cloud, computing.

INTRODUCTION

The growing popularity of cloud computing increases security concerns for many users. As more content moves to the cloud versus being stored locally, where users carry the majority of the burden of ensuring the security of their content the security demands of cloud service providers becomes more important. Users need to be assured their content is secure. It is critical for organizations to control and customize security in cloud services. Commonly used productivity tools that require security include:

- Email
- Calendars
- Content management
- Collaboration
- Unified communications

IT teams are required to deliver access to services from more devices, platforms, and places than ever before. Clearly, multi-device access to corporate assets benefits users, but broader access makes security management more challenging. Each endpoint represents a potential attack surface and another point management for security professionals. At the same time, organizations face ever-evolving threats from around the world.

Organizations expanding remote access while maintaining security best practices may find it difficult and expensive to add this combination of security functionality if they deploy productivity services solely on- premises.

Security Mechanism and topologies

An in-depth strategy ensures that security controls are present at various layers of the service and that, should any one area fail, there are compensating controls to maintain security at all times. The strategy also includes tactics to detect, prevent, and mitigate security breaches before they happen. This involves continuous improvements to service-level security features, including:

Port scanning and intermediation

- Perimeter vulnerability scanning
- Operating system security patching
- Network-level distributed denial-of-service (DDoS) detection and prevention
- Multi-factor authentication for service access

For more information on how Office 365 is protected against DDoS attacks, see Defending Office 365 against denial of service attacks, available for download from the Service Trust Portal (STP). Note, you must be enrolled in the STP to access this document. Enrolment is free and easy for all Office 365 tenants (including trial subscriptions).

With regards to people and process, preventing breaches involves:

Auditing all operator/administrator access and actions

- Zero standing permission for administrators in the service
- Just-In-Time access and elevation that is granted on an as-needed and only-at-the-time-of-need basis to troubleshoot the service
- Segregation of the employee email environment from the production access environment

Office 365 data is stored in the Microsoft network of data centres, run by Microsoft Global Foundation Services and strategically located around the world. These data centers are built from the ground up to protect services and data from harm by natural disaster or unauthorized access. Data centre access is restricted 24 hours per day by job function so that only essential personnel have access to customer applications and services. Physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication.

Isolated Data Network

One reason Office 365 is both scalable and low cost is that it is a multi-tenant service (that is, data from different customers shares the same hardware resources). Office 365 is designed to host multiple tenants in a highly secure way through data isolation. Data storage and processing for each tenant is segregated through Active Directory structure and capabilities specifically developed to help build, manage, and secure multi-tenant environments. Active Directory isolates customers using security boundaries (also known as silos). This safeguards a customer's data so that the data cannot be accessed or compromised by co-tenants. For additional cost, a version of Office 365 that stores data on dedicated hardware is available.

Secure channels

Networks within the Office 365 data centers are segmented to provide physical separation of critical back-end servers and storage devices from the public-facing interfaces. Edge router security allows the ability to detect intrusions and signs of vulnerability. Customer access to services provided over the Internet originates from users' Internet-enabled locations and ends at a Microsoft data center. These connections are encrypted using industry-standard transport layer security (TLS)/ SSL. The use of *TLS/SSL establishes a highly secure client-to-server connection* to help provide data confidentiality and integrity between the desktop and the data center.

Admin access to Encrypted Data

Administrator access to Office 365 and your data is strictly controlled. Core tenets of this process are role based access and granting personnel least privilege access to the service that is necessary to perform specific operations. These tenets are followed whether the access is physical (i.e., to the datacenter or the servers) or logical. An example where this comes to life is a process called "Lock box" that administrators use to request access for elevated privileges.

Access control happens at various levels:

Personnel level to ensure that there are appropriate background checks and strict account management so that only those essential to the task may perform the task.

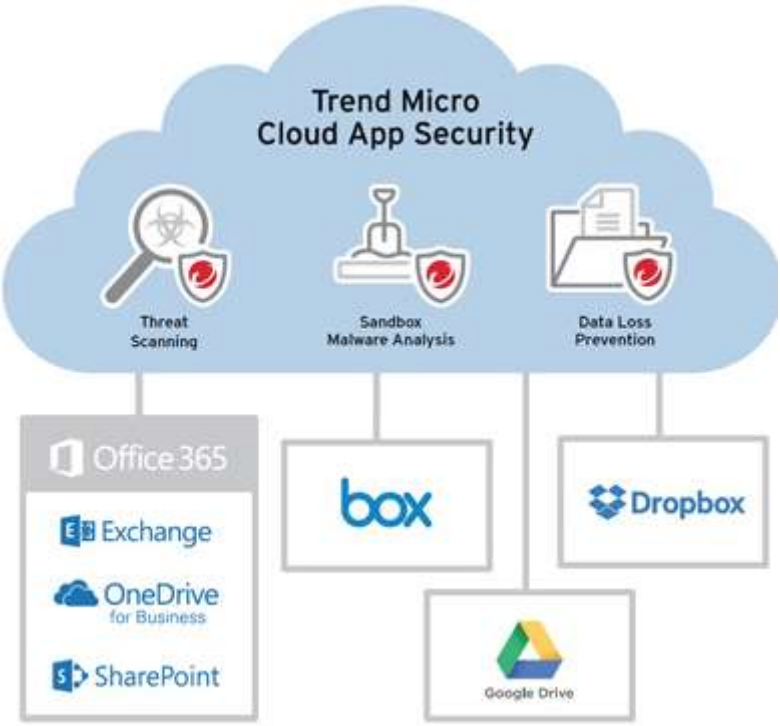

Fig. 1: Cloud App Security and mechanism

The above explains the security layers of 0365:

A defense-in-depth strategy ensures that security controls are present at various layers of the service and that, should any one area fail, there are compensating controls to maintain security at all times. The strategy also includes tactics to detect, prevent, and mitigate security breaches before they happen. This involves continuous improvements to service-level security features, including:

- Port scanning and remediation
- Perimeter vulnerability scanning
- Operating system security patching
- Network-level distributed denial-of-service (DDoS) detection and prevention
- Multi-factor authentication for service access

For more information on how Office 365 is protected against DDoS attacks, see Defending Office 365 against denial of service attacks, available for download from the Service Trust Portal (STP). Note, you must be enrolled in the STP to

access this document. Enrollment is free and easy for all Office 365 tenants (including trial subscriptions). See Get started with the Service Trust Portal for Office 365 for business, Azure, and Dynamics CRM Online subscriptions for steps to enroll.

With regards to people and process, preventing breaches involves:

- Auditing all operator/administrator access and actions
- Zero standing permission for administrators in the service
- Just-In-Time access and elevation that is granted on an as-needed and only-at-the-time-of-need basis to troubleshoot the service
- Segregation of the employee email environment from the production access environment
- Mandatory background checks for high-privilege access. These checks are a highly scrutinized, manual-approval process.

Preventing breaches also involves automatically deleting unnecessary accounts when an employee leaves, changes groups, or does not use the account prior to its expiration. Wherever possible, human intervention is replaced by an automated, tool-based process, including routine functions such as deployment, debugging, diagnostic collection, and restarting services.

We continue to invest in systems automation that helps identify abnormal and suspicious behavior and respond quickly to mitigate security risk. We are also continuously evolving a highly effective system of automated patch deployment that generates and deploys solutions to problems identified by the monitoring systems—all without human intervention. This greatly enhances the security and agility of the service. We regularly conduct penetration tests to enable continuous improvement of incident response procedures. These internal tests help our security experts create a methodical, repeatable, and optimized stepwise response process and automation.

Physical Layer – Facility

Customer data is stored in our Office 365 datacenters that are geographically distributed while taking regional data location considerations into account. Our datacenters are built from the ground up to protect services and data from harm by natural disaster or unauthorized access. Datacenter access is restricted 24 hours a day by job function—with only customer application and services access given to essential personnel. Physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication. The datacenters are monitored using motion sensors, video surveillance, and security breach alarms. In case of a natural disaster, security also includes automated fire prevention and extinguishing systems and seismically braced racks where necessary.

Physical Layer – Network

Perimeter protection is implemented through the use of controlled devices at the network edge and on points throughout the network. The overarching principle of our network security is to allow only connections and communications that are necessary to allow systems to operate, blocking all other ports, protocols and connections. Access Control Lists (ACLs) implemented in the form of tiered ACLs on routers, IPsec policies on hosts, firewall rules and host based firewall rules are implemented in the network with restrictions on network communication, protocols, and port numbers. Edge router security allows the ability to detect intrusions and signs of vulnerability at the network layer. Networks within the Office 365 datacenters are further segmented to provide physical separation of critical back-end servers and storage devices from the public-facing interfaces.

RELATED WORK

- Reduces risk of spear-phishing emails and protects file sharing: Extends Microsoft's built-in anti-malware with pattern-less malware detection using sandbox analysis to open files in a virtual environment and detects malicious behaviour
- Uncovers hidden malware in Office files: Uses document-exploit detection to find hidden malware inside common Office file formats such as Word, Power Point, and Excel. Trend Micro found this method of infiltration

in 60% of targeted attacks in a recent report.

- Enforces compliance for cloud file-sharing services: Controls sensitive data usage with DLP protection for Box, Drop box, Google Drive, Share Point On-line, and One Drive for Business with more than 200 pre-built and customizable compliance templates.
- Keeps collaboration free from infiltration: Scans files shared by remote workers and partners, and from mobile devices, to ensure threats can't use internal email or cloud file-sharing services to migrate.
- Deploys automatically with no software or device changes: Cloud-to-cloud API integration doesn't rely on redirecting email or setting up web proxies.

System requirements

Cloud applications	Details
Office 365	Office 365 Education, Business, or Enterprise
Box	Box Business and Enterprise
Drop box	Drop box Business
Google Apps for Work	Supports Google Drive within Google Apps for Work. (Trend Micro Hosted Email Security can provide additional email protection)

Cloud App Security is now part of the Trend Micro Smart Protection Complete Suite. This connected, multi layered security suite protects your users and their data regardless of what device they use or where they are working. The Smart Protection Complete Suite combines the broadest range of endpoint and mobile threat protection capabilities with multiple layers of email, collaboration, and gateway security. And it enables you to manage users across multiple threat vectors from a single management console that gives you complete user-based visibility into the security of your environment.

APPROACHES

Microsoft security best practices

Security in Office 365 is an ongoing process, not a steady state. It is constantly maintained, enhanced, and verified by experienced and trained personnel, and Microsoft strives to keep software and hardware technologies up to date and refined through robust designing, building, operating, and supporting processes. To help keep Office 365 security the best in the industry, Microsoft uses processes such as Security Development Life-cycle; traffic throttling; and preventing, detecting, and mitigating breach.

Security development life cycle

Security at Microsoft begins before the public ever hears of a particular application or service. The Microsoft Security Development Life-cycle (SDL) is a comprehensive security assurance process that informs every stage of design, development, and deployment of Microsoft software and services, including Office 365. Through design requirements, analysis of attack surface, and threat modelling, the SDL helps Microsoft predict, identify, and mitigate vulnerabilities and threats from before a service is launched through its entire production life cycle. Microsoft continuously updates the SDL using the latest data and best practices to help ensure that new services and software associated with Office 365 are highly secure from day one.

Traffic throttling to prevent denial-of-service attacks

Exchange On-line tracks usage baselines and accommodates normal traffic bursts without affecting the user experience. When traffic from a user exceeds typical parameters, that traffic is throttled until usage returns to normal. Whether the excessive traffic is caused by user behaviour or a malicious attack such as a denial-of-service, Exchange automatically responds to help ensure that other users are not affected.

Key trends affecting Security

- Consmerization of IT
- Targeted Attacks
- Identity Centric Environment
- Cloud Computing
- Regulatory / Compliance issues

Cloud Security Alliance

Office 365 fulfils compliance and risk management requirements as defined in the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM). The CCM is published by a not-for-profit, member-driven organization of leading industry practitioners focused on helping customers make the right decisions when moving to the cloud. The matrix provides a detailed understanding of the security and privacy concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains. Office 365 has published a detailed overview of its capabilities for the CCM requirements that illustrates how these capabilities meet these requirements and empowers customers with in-depth information to evaluate different offerings in the marketplace today.

CONCLUSION

Office 365 is a robust and capable cloud-based offering that can satisfy the email, real-time communications, document sharing, collaboration and document creation needs of small, midsized and large organizations. However, despite the many features baked into Office 365, it will not satisfy every requirement, particularly in the context of highly regulated organizations or those with specialized security needs. Information regarding Office 365 security, privacy, compliance, transparency, and service continuity can be found in the Office 365 Trust Center. The Office 365 platform incorporates security at every level, from application development to physical data centers to end-user access. Today, fewer and fewer organizations have the ability to maintain an equivalent level of security on-premises at a reasonable cost.

REFERENCES

[1]. https://products.office.com/en/business/office-365-trust-center-welcomehttps://products.office.com/en/business/office-365-trust-center-welcome

[2]. Office 365 collaboration and co-authoring

[3]. Rob Efferents, General Manager, Extensibility at Microsoft

[4]. https://www.skyhighnetworks.com/product/office-365-security/

[5]. http://www.oit.uci.edu/office365-project/risk-summary/

[6]. Benjamin Niaulin - Author
[7]. http://en.share-gate.com/guides/office-365-security

[8]. Ara M. -Author
[9]. https://kb.wisc.edu/office365/page.php?id=34730