happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

# ENTERPRISE-GRADE SECURITY IN MICROSOFT OFFICE 365:

# BEST PRACTICES & TECHNOLOGIES

# INTRODUCTION

Microsoft Office 365 is a SaaS solution designed with next-gen cloud-based communications and collaboration services like Microsoft Exchange Online, Microsoft SharePoint Online, Skype for Business Online, Microsoft Teams and more. It effectively delivers the power of cloud productivity to the organization regardless of size and thus resulting in time and cost reduction Today, "Data is the New Gold". Moving your organization to cloud that is hosted on the network of an external service provider adds another layer of concern for data protection and Security. Microsoft, however, takes these concerns very seriously and have applied their years of experience to equip Office365 with world-class Privacy and Compliance features for securing the on-premise or cloud infrastructure. Microsoft Office 365 services can help to get the benefits of cloud computing with the enterprise-grade Security irrespective of the size of the organization.

# SECURITY CHALLENGES

Microsoft Office 365 platform leverage the users to access their services and data from around the globe using any device over the internet. With such a high risk of access to the data that attract hackers, causing a severe threat to your data system that initially goes undetected. Nowadays Cybercrime is operated by highly skilled, organized and professional attackers.

In this competitive world, we have seen a rapid growth of the organizations, so as business data and hence the need for a comprehensive approach to security is a must to secure the data. Along with all these data backup, storage and Data recovery become major cost centers for IT Department. Hence, the organizations start looking for a secure, affordable, scalable solution for ensuring Security and round the clock availability.

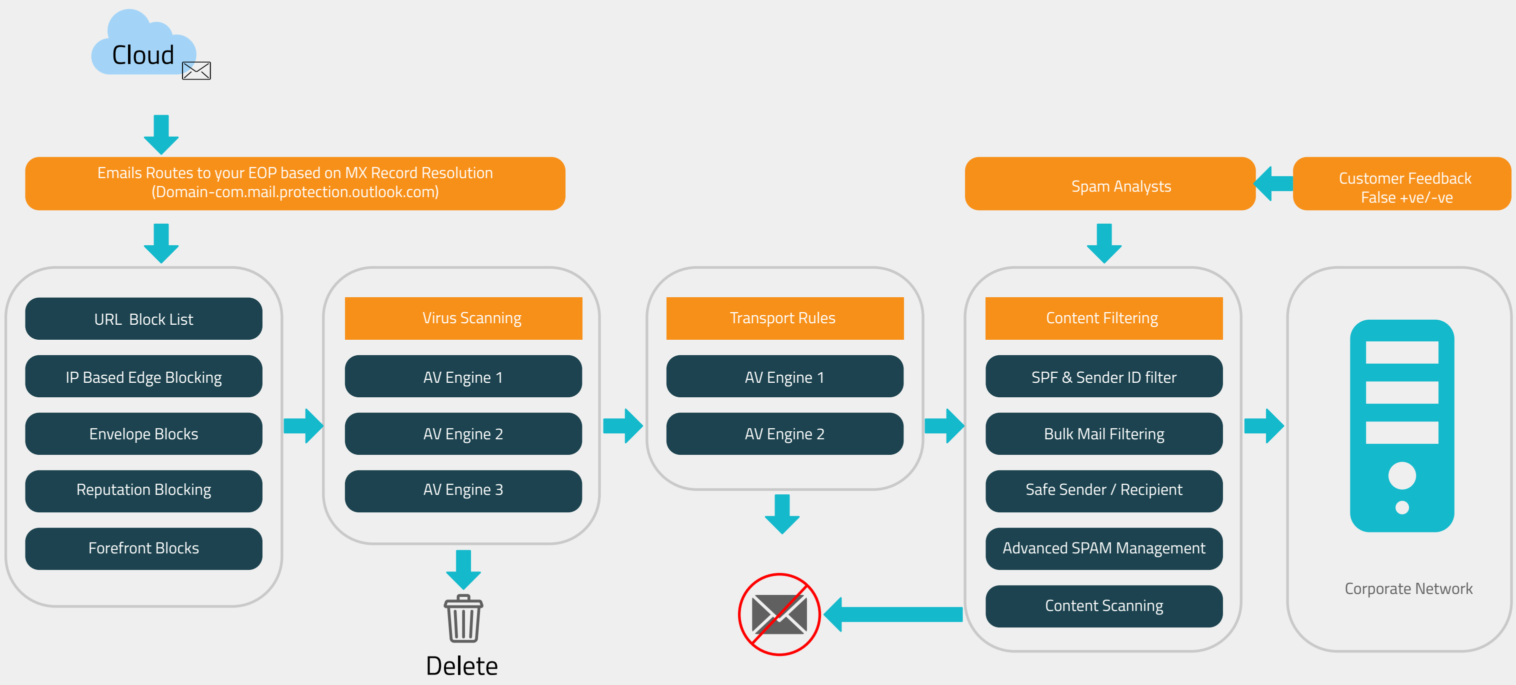
# SECURITY AND COMPLIANCE

Security and compliance is not a onetime setup process it requires constant maintenance, up-gradation and enhancement of the security requirements keeping the flow of work up to date plus detecting and mitigating threats at the early stage helps to create a secure environment.

Office 365 is a multi-tenant service, which means that Office 365 customers share the Datacenter space with other multiple organization. Still, Data Storage and Data processing are logically segregated between customers through advanced Active Directory technology. This is one of the reasons that Office 365 provide Cost and scalability benefits.

## Exchange Online Protection Inbound Security Filtering Overview

Using EOP is a mandate with Office 365 Platform, an Edge service, which means something that exists between your network and internet and sits outside your system. EOP provides robust email protection against SPAM, Malware and Viruses before entering any email inside the network. It is a sum-up of processors and filters, some of which are native to Exchange, Some from Microsoft Forefront Gateway. EOP perform tasks in various stages some as per pre-defined database value, some as per e-mail content and some as per security policy created in an environment.



## Connection Filtering

Any email that routes to your organization based on Mx-record resolution pass through multiple check posts.

**Real-Time Blocklist: -** Microsoft maintains a database that keeps track of mail server IP addresses and senders with a bad reputation/spammer list as well. Any email from those IP's gets deleted before entering the environment.

**URL Block Lists: -** EOP includes 750,000+ domains of known Spammers and uses several URL blocks lists to detect the known malicious link within Messages.

**Virus Scanning: -** On passing the first stage email gets scanned by 3 Anti-Virus Scanners for malware and delete the suspected emails.

## Content Filtering

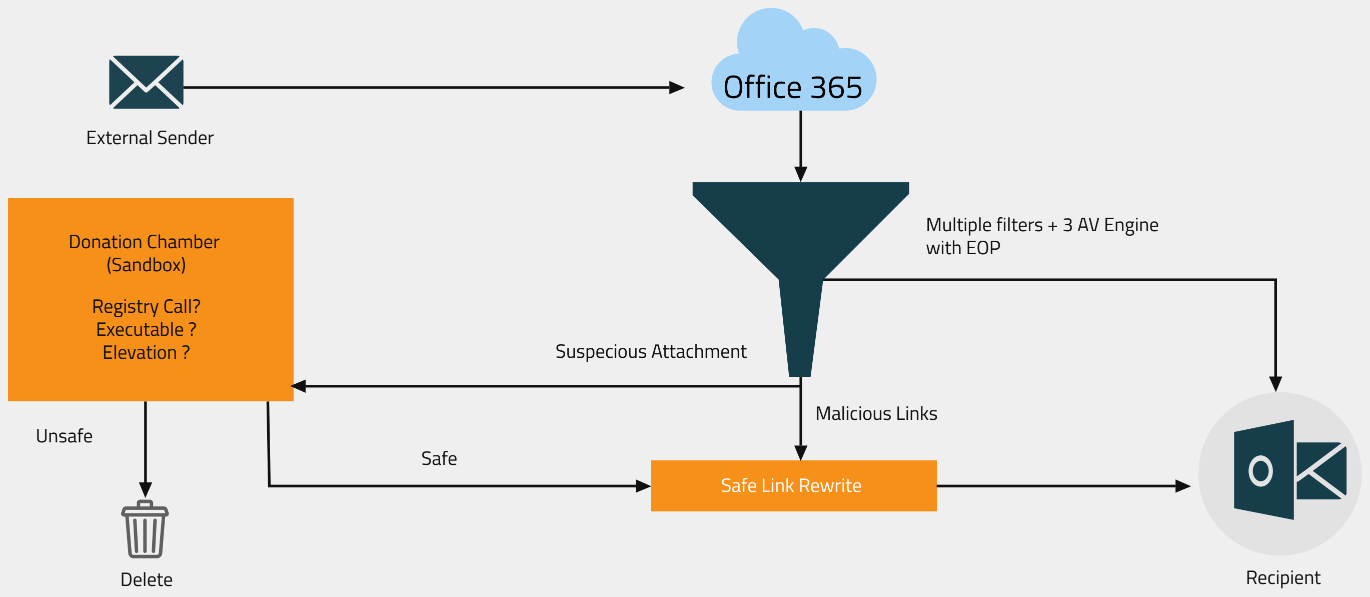
This gives the ability to Admins to configure and manage policy for Spam filtering.

**Custom Rules: -** Admins can create custom content filter policies and apply them to a specified User, Group, Sender IP, Domains ex- Blacklist, Whitelist, and more. Configure actions on content Filtered Messages.

**Spam Protection: -** Emails Content gets analyzed against the custom policies like the Spam Confidence Level (SCL), Bulk Confidence level (BCL) etc. and configure actions on Content Filtered Messages.

# Advanced Threat Protection

With advancement in technology, spammers also become more organized and launch increasingly sophisticated attacks and hence most organizations now seeking more advanced security protection. To achieve this, Microsoft offers advanced threat protection, a smarter email filtering service that provides additional protection against powerful email attacks and threats.



(ATP SCAN ENGINE)

Exchange Online Advanced Threat Protection Delivers given below Benefits: -

**ATP Safe Attachment: -** This feature is the extended and advanced version of EOP 3-layer AV scan Engine. EOP AV Scan Engine protects against known viruses and malwares, wherein this protection gets the extend by scanning all the emails that don't have known virus/malware in a separate virtual (Hypervisor) environment and provide better protection to safeguard your environment. If no suspicious activity is detected, the messages are released to the mailbox.

**ATP Safe Link: -** This is again an extended feature to EOP, which scans and access every URL in the message in virtual (Hypervisor) environment and blocks if any URL redirects to Unsafe website. ATP's safe link feature proactively protect users if they click any such link.

**Rich Reporting and URL Tracing: -** ATP also offers to report and tracing a capability, that leverage you to check and investigate the messages that have been blocked due to Unknown virus or malware.

## Data Loss Prevention

DLP is one of the features of **Office 365** that is a set of tools and processes used to ensure that sensitive data is not misused, shared outside organization or accessed by unauthorized users. DLP is extremely helpful in protecting personally identifiable information such as **credit card number, bank account, driving license numbers** and more. and comply with regulations. DLP Policies are Transport Rules (Condition, Exceptions and Actions), created and managed by both exchange admin center and PowerShell Cmdlets.

## eDiscover

One of the key features of **Office 365** Compliance Center, which helps in searching, identifying and delivering required data electronically that can be used for restoring old data for end-user or Legal Purpose. This feature eases the functionality of searching data per different conditions (ex- Sender, Recipient, Message-ID, Date & Time, Keywords/Phrases etc.) in Exchange Online, SFB online, MS Teams, SharePoint Online and OneDrive Documents. To perform eDiscovery search, a user has been a member of the Management role group or a global admin as because by default, no one in the environment has the rights to access eDiscovery center and cases. eDiscovery searches and cases that can be managed by both office 365 Security & Compliance Center and PowerShell CmdLets.

## Auditing and Retention policies

The audit log information is vital for most of the businesses due to legal or compliance requirements, and so does for the exchange admins to keep track of who performed what tasks across the environment. Office 365 provides extensive Audit logging which means you can find user and admin logs details for Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, MS Teams, Azure AD, Power BI, Sway, eDiscovery, Dynamics 365 etc. Audit Logs can be searched by different Filters like users, day and time, user roles etc. and Audit Logs are retained up to 90 days.

Retention of Emails, Chats and documents are required for legal, Business or compliance reasons or to remove emails/chats that aren’t required to retain. Office 365 provides the records management technology MRM (Messaging records management) that enables the age of Items in Mailboxes and define the actions to take on Items upon reaching a specified period

Below Retention Tags and Policies are used in Office 365 to accomplished MRM: -

Retention Policy Tag (RPT): Assigned to Default Folders, ex-Inbox, Sent Items, Deleted Items.

Default Policy Tag (DPT): Assigned to all the Untagged Items (DPT is applied by default If no Policies is applied)

Personal Tag: Assigned to Custom Folders (folders created by uszers)

## Lockbox

Office 365 offers an extremely important feature through which users can control how a Microsoft Engineer is going to access their data during a scenario where user raised a Support Request with Microsoft to investigate service-related issue and screen sharing is required. The Lockbox allows users to Approve or Reject Machine access request made by Microsoft Support engineer.

## Secure Transport and Authentication Methods

It is the key Feature of Office 365 to achieve this Exchange Online Uses Opportunistic TLS. EXO always tries to Encrypt Connection with the Latest version first, then look it is way down the list of TLS cyphers until it finds one on which both sending and receiving parties can agree.

Office 365 uses cloud-based Azure AD, (included in Office 365 subscription) to manage identities and authentication in cloud. But It also leverages you to implement On-Premise federation services (ADFS) to perform authentication and act as a Source of Authority (SOA). After federation is configured, all Office 365 users whose identities are based on the federated domain can use their existing On-Premise logons to authenticate to Office 365. ADFS enables token-based authentication. ADFS also allows administrators to create additional authentication Methods such as: -

Single Sign-on: SSO is related to the authentication part of federated identity, and it is a user authentication service that permits the user to use the same set of login credential to access multiple Application.

Multi-Factor Authentication: Multi-factor authentication enhances Security in a multi-device and cloud-centric world. Office 365 provides an in-house solution for multi-factor authentication with a phone call, SMS, notification on a dedicated app. Office 365 also leverage integration with third-party MFA tools.

# Conclusion

In this Competitive world, organizations need productive services that leverage users to work from anywhere while maintaining security. Office 365 fulfil both requirements with Secure and cloud-based productivity platform. Office 365 designed to deliver the enterprise-grade security you require to move to the cloud with confidence. Office 365 helps the user & administrators from accessing the data and services with the best security practice that make sense for their unique business needs.

# Author Bio:

*"Rohan has got 7.6 years of experience in Infra - IT with expertise in MS Exchange, Office 365, G-Suite Migrations, Operational support on Enterprise Messaging. He has exposure to Messaging and Collaboration platform that covers his expertise in design, build & deploy, and Support Office 365, Google Suite. He is currently a part of EUCS Practice and responsible for writing Technical Proposals, planning and executing migrations on different messaging cloud platform."*

Business Contact **business@happiestminds.com**

## About Happiest Minds Technologies

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transfor-mation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in the U.S., UK, The Netherlands, Australia and Middle East.

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

www.happiestminds.com