## Contents

Exchange Online Advanced Threat Protection ................................................................. 3
Solution overview ............................................................................................................. 4
Service architecture ......................................................................................................... 5
Safe Attachments ............................................................................................................. 6
Safe Links .......................................................................................................................... 8
Reporting and tracing ....................................................................................................... 9
How to buy Exchange Online Advanced Threat Protection ............................................. 11
Exchange Online Advanced Threat Protection

Microsoft Office 365 provides robust email protection against spam, viruses, and malware with Microsoft Exchange Online Protection (EOP). But as hackers around the globe launch increasingly sophisticated attacks, organizations are seeking tools that provide additional protection. We are pleased to offer customers new security capabilities in Office 365 with Exchange Online Advanced Threat Protection (ATP), an email filtering service that provides additional protection against specific types of advanced threats.
Solution overview

Exchange Online Advanced Threat Protection is a cloud-based email filtering service that helps protect your organization against unknown malware and viruses by providing robust zero-day protection. ATP includes features to help safeguard your organization from harmful links in real time. It also has rich reporting and URL trace capabilities that give admins insight into the kind of attacks happening in your organization.

ATP for Exchange Online delivers the following benefits:

- **Protection against unknown malware and viruses.** Today EOP employs robust and layered antivirus protection powered with three different engines against known malware and viruses. ATP extends this protection through a feature called Safe Attachments, which helps protect against unknown malware and viruses and provides better zero-day protection to safeguard your messaging system. All messages and attachments that don’t have a known virus/malware signature are routed to a special hypervisor environment, where a behavior analysis is performed using a variety of machine-learning and analysis techniques to detect malicious intent. If no suspicious activity is detected, the message is released for delivery to the mailbox.

- **Real-time, time-of-click protection against malicious URLs.** EOP scans each message in transit in Office 365 and provides time of delivery protection, blocking malicious hyperlinks in a message. But attackers sometimes try to hide malicious URLs within seemingly safe links that are redirected to unsafe sites by a forwarding service after the message has been received. The ATP Safe Links feature proactively protects your users if they click such a link. That protection remains every time they click the link, so malicious links are dynamically blocked while good links can be accessed.

- **Rich reporting and URL trace capabilities.** ATP also offers rich reporting and tracking capabilities, so you can gain critical insights into who is getting targeted in your organization and the category of attacks you are facing. Reporting and message tracing allows you to investigate messages that have been blocked due to an unknown virus or malware, while the URL trace capability allows you to track individual malicious links in the messages that have been clicked.
Exchange Online Advanced Threat Protection capabilities:

- **Safe Links**—proactively protects your users from malicious hyperlinks in a message. The protection remains every time they click the link, so malicious links are dynamically blocked while good links can be accessed.

- **Safe Attachments**—helps protect against unknown malware and viruses, and provides zero-day protection to safeguard your messaging system. All messages and attachments that don’t have a known virus/malware signature are routed to a special environment where ATP uses a variety of machine-learning and analysis techniques to detect malicious intent. If no suspicious activity is detected, the message is released for delivery to the mailbox.

- **Dynamic Delivery**—a Safe Attachments feature that reduces latency of message delivery while an attachment is being inspected for malware.
Safe Attachments

Safe Attachments is a feature that opens suspected unknown attachments in a special hypervisor environment and detects malicious activity. It is designed to detect malicious attachments even before anti-virus signatures are available. Safe Attachments detonates attachments that are common targets for malicious content, such as Office documents, PDFs, executable (EXE) files, and Flash files.

What is Dynamic Delivery of Safe Attachments?

Dynamic Delivery is an innovative feature and a differentiated capability. After going through the standard Office 365 protection process of multiple antivirus engines and multiple spam filters, an email with a suspicious attachment enters the Safe Attachments sandbox environment, which has a detonation chamber to analyze the attachment and determine whether or not it’s safe—a process that takes an average of four minutes (up to 30 minutes, depending on file type).

With Dynamic Delivery of Safe Attachments, that delay is eliminated by sending the body of the email with a placeholder attachment, while the actual suspicious attachment undergoes a Safe Attachments scan. Recipients can read and respond to the message, which includes notification that the original attachment is being analyzed. If the real attachment is cleared, it replaces the placeholder; if not, the admin can filter out the unwanted and potentially malicious attachment.
Set up a Safe Attachments policy

1. In the Exchange Admin Center (EAC), go to Advanced threats > Safe attachments, and then assign a name to your policy.

2. Select the action you want at your organization for unknown malware in attachments: either Monitor, Block, or Replace.

3. Under Redirect attachment on detection, select Enable redirect and enter an email address to receive the ATP notification.

   Microsoft recommends creating a new mailbox to receive ATP notifications because these notifications will contain the attachments detected as unknown malware.

4. To enable an attachments policy that can be applied to users, groups, and domains in your organization, go to the Applied to section of the ATP policy, and then choose The recipient is, The recipient domain is, or The recipient is a member of.

5. Save your policy.
Safe Links

Safe Links is a feature that helps prevent users from going to malicious websites when they click them in email. Safe Links has advanced reporting features that make it easy to determine who has clicked through to a malicious link, which supports faster remediation.

Set up a Safe Links policy

6. In the Exchange Admin Center (EAC), go to **Advanced threats > Safe links**.
7. Go to **Settings**, and then choose **On** so that URLs will be rewritten and checked.
8. Optional: Clear the **Do not track user clicks** check box if you don’t want to store information about which user followed a particular link. Select the check box to store this information.
9. Optional: Clear the **Do not allow users to click through to the original URL** check box if you want your users to have the option of following a link even if ATP has determined that the link points to a malicious website. Select the check box to stop users from proceeding to the URL target of a link.
10. Choose **Save**.
Reporting and tracing

Find out whether a specific email has been detonated, and get the results. And find out who has been following malicious links.

Message Trace

With the Message Trace feature, you can keep track of each message and attachment that is routed to Safe Attachments after a policy is applied. To find out the status of such messages, go to the Exchange Admin Center and choose mail flow > message trace. The Message Trace details have information for each message and attachment.

URL Trace

Your Safe Links policy can be enabled to log which recipients are following links that have been protected by Safe Links. If tracking URLs is also enabled, this information can be found in the Exchange Admin Center by choosing mail flow > URL trace. You can sort the URL Trace report by date range, recipients, and specific URLs.
View ATP Disposition Reports

The disposition reports created by ATP can be used to see the number of messages and file types routed to Safe Attachments.

1. In the Exchange Admin Center (EAC), go to Advanced threats.
2. Click the reports icon arrow, and choose to view the Advanced Threat Protection Disposition Report by either file type or disposition.

Zero-hour Auto Purge

If an unread email is incorrectly categorized as spam, malicious, or safe, Zero-hour Auto Purge provides the ability to change that verdict. For example, if a message is delivered to your Inbox and later found to be spam, Zero-hour Auto Purge moves that message from the Inbox to the spam folder; the reverse is true for messages misclassified as spam. Admins have total control over whether or not to use this feature, because Zero-hour Auto Purge can be disabled in the EAC.
How to buy Exchange Online Advanced Threat Protection

Protect your email in real time against unknown and sophisticated attacks.

Advanced Threat Protection is included in the most comprehensive enterprise plan: Office 365 Enterprise E5.

You can also add Advanced Threat Protection to the following Exchange and Office 365 subscription plans for $2.00 per user per month: Exchange Online Plan 1, Exchange Online Plan 2, Exchange Online Kiosk, Exchange Online Protection, Office 365 Business Essentials, Office 365 Business Premium, Office 365 Enterprise E1, Office 365 Enterprise E2, Office 365 Enterprise E3, Office 365 Enterprise E4, Office 365 Enterprise K1, Office 365 Enterprise K2.

To add Advanced Threat Protection to your subscription, contact your volume licensing reseller or visit office.com/enterprise-solutions to learn more.