Exchange Online Advanced Threat Protection

Product Guide

Microsoft

Contents

Exchange Online Advanced Threat Protection

Office 365 provides robust email protection against spam, viruses, and malware with 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

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

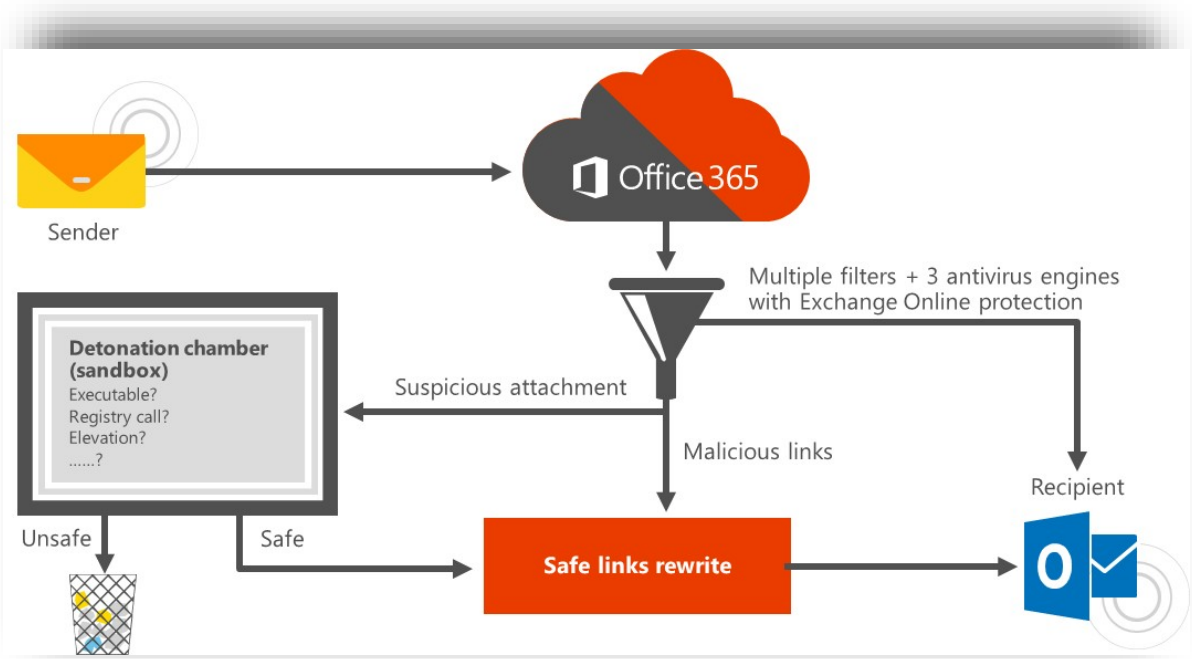
Advanced Threat Protection for Exchange Online delivers the following benefits:

- Protection against unknown malware and viruses—Today EOP employs a robust and layered anti-virus 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 with seemingly safe links that are redirected to unsafe sites by a forwarding service after the message has been received. ATP's Safe Links feature proactively protects your users if they click such a link. That protection remains every time they click the link, as 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.

Service Architecture



Exchange Online Advanced Threat Protection Capabilities:

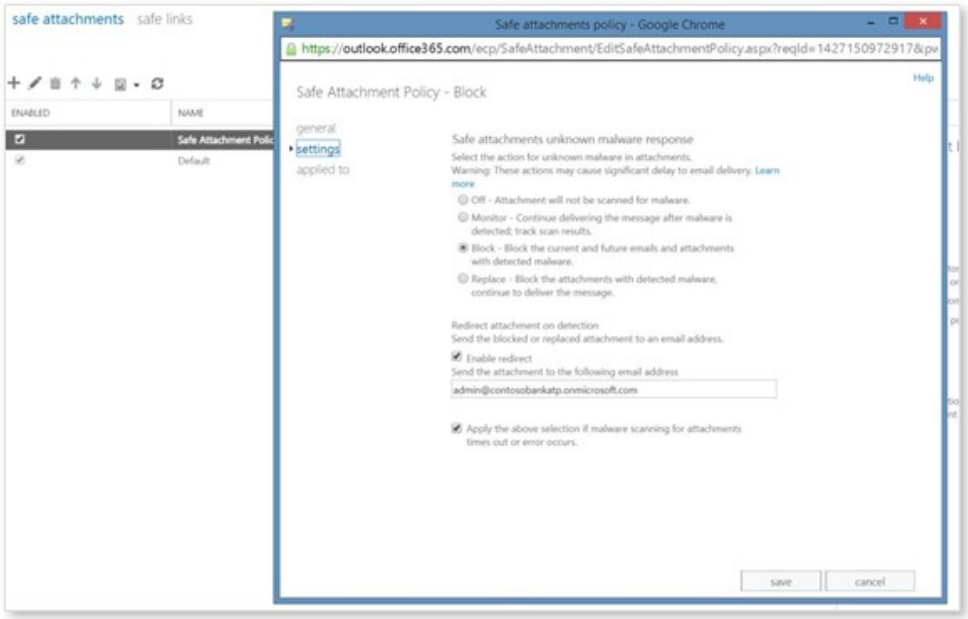
- Safe Links
  ATP's Safe Links feature proactively protects your users from malicious hyperlinks in a message. The protection remains every time they click the link, as malicious links are dynamically blocked while good links can be accessed.

- Safe Attachments
  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.

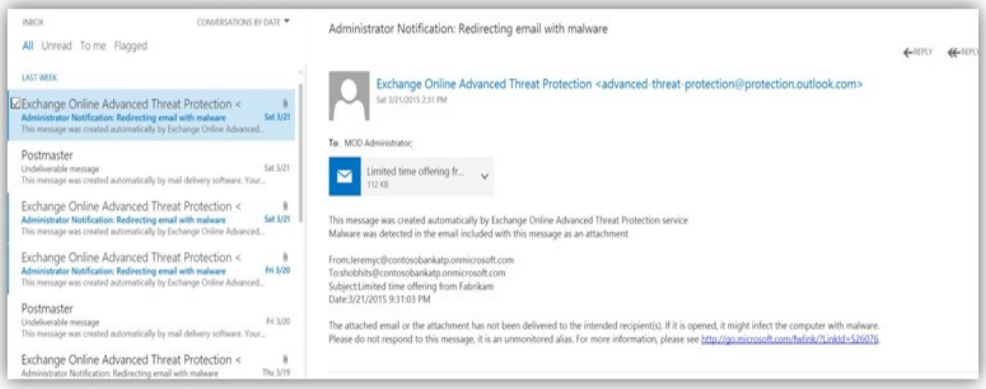
Safe attachments

What is Safe Attachments?

Safe Attachments is a new feature that opens suspected unknown attachment 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 will detonate attachments that are common targets for malicious content, such as Office documents, PDFs, executable file types, and Flash files.



Admin sets policy



Admin gets notification if message is blocked

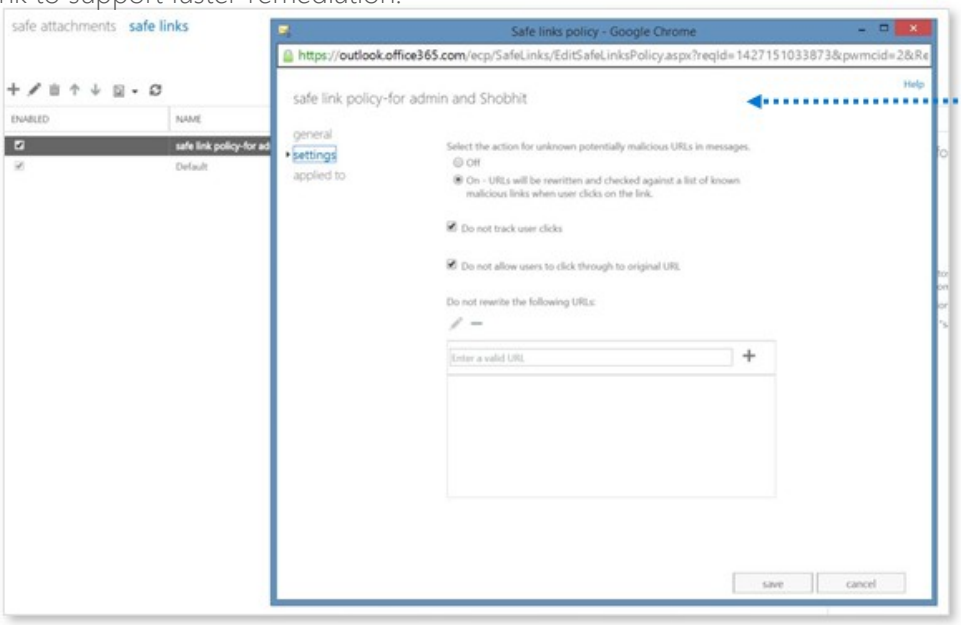
Set up a safe attachments policy

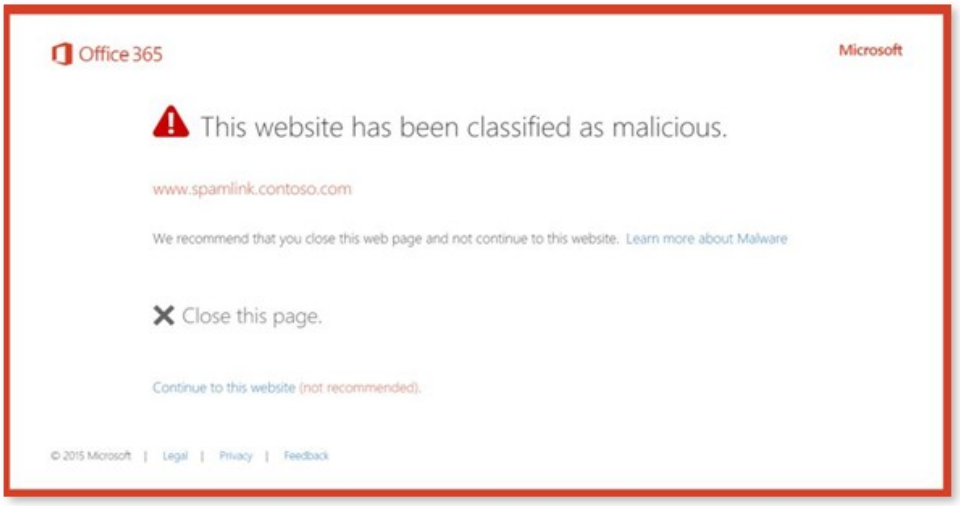
1. In the Exchange Admin Center (EAC), go to Advanced threats > Safe attachments. (Name your policy)
2. Select the action for unknown malware in attachments: Monitor, Block or Replace
3. Configure the Redirect attachment on detection and enter in an email address to receive the ATP notification. *It is recommended creating a new mailbox to receive ATP notifications since they will contain the attachment detected as unknown malware.
4. If you want 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 if a member of.
5. Save your policy

Safe Links

What is Safe Links?

Safe Links is a feature that prevents users from going to malicious web sites when they click on them in email. Safe Links has advanced reporting features that make it easy to determine who has clicked through a malicious link to support faster remediation.





Setup a Safe Links Policy

1. In the Exchange Admin Center (EAC), go to Advanced threats > Safe links.
2. Go to Settings, and then choose On so that URLs will be rewritten and checked.
3. Optional: Uncheck Do not track user clicks if you don't want to store information about which user followed a particular link. Do check the box if you want to store this information.
4. Optional: Uncheck Do not allow users to click through to the original URL 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. Do check the box in order to stop users from proceeding to the URL target of a link.
5. 5.Choose Save.

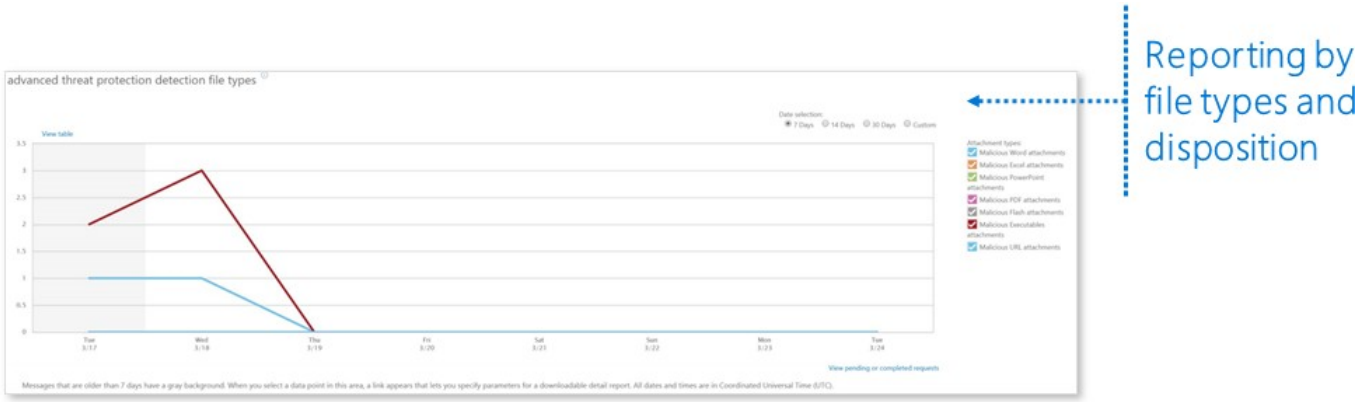
Reporting and Tracing

Message Trace

Find out if a specific email has been detonated, and get the results - 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

Find out who has been following malicious links - 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.



ATP Disposition Reports

The disposition reports can be used to see the number of messages and file types

1. To access the disposition reports, in the Exchange Admin Center (EAC), go to Advanced threats > Click the reports icon drop down arrow to select either the Advanced Threat Protection Disposition Report by file type or disposition.

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 new, 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: 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.