

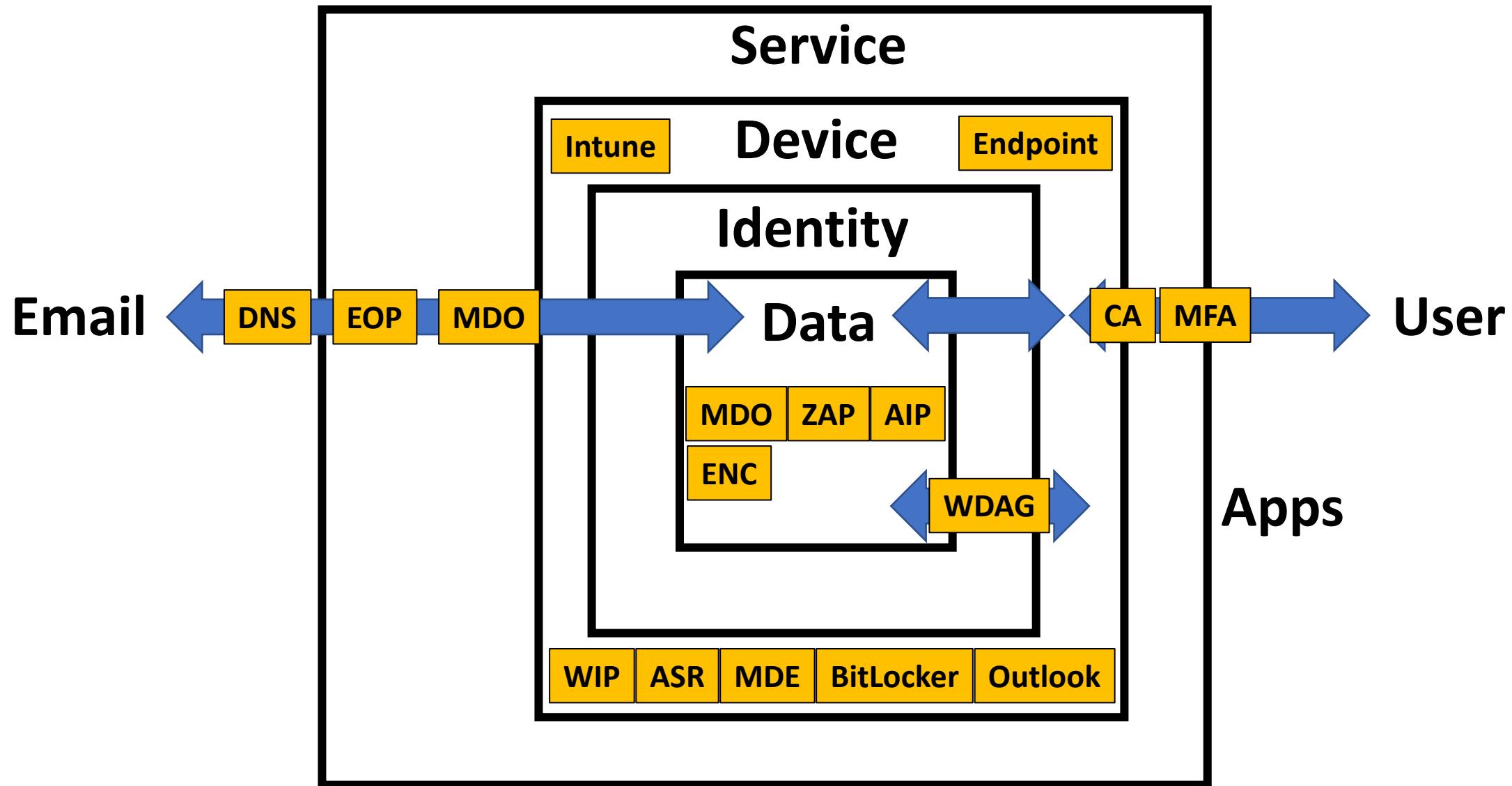


CSP Masters Program in person series

Technical training



Email Security





How can I secure my customer's e-mail solution?

Name: Megan B

Role: Partner Resource

Company: Partner



The basics



Exchange Online Protection (EOP)

Blocks commodity spam and malware



Transport Rules

Block auto-forward

Add warnings



DNS records

MX, SPF, DKIM, & DMARC



Defender for Office 365

Analyzes email & files for anything suspicious



EOP & Defender for Office 365

Does not address endpoint or network security

Email Protection



Exchange Online Protection (EOP)

Blocks commodity spam and malware



Transport Rules

Block auto-forward
Add warnings

The basics



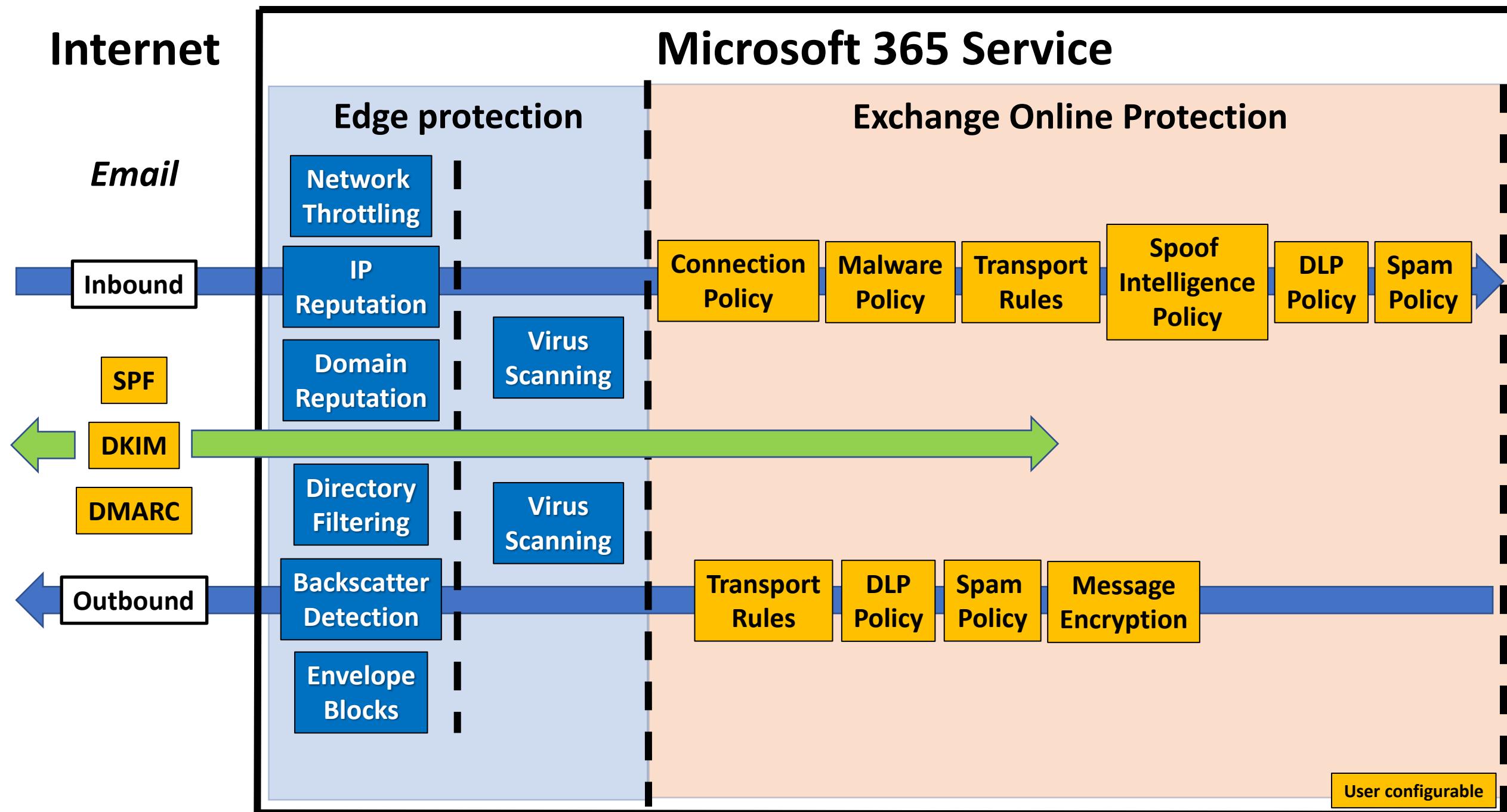
DNS records

MX, SPF, DKIM, & DMARC

Internet

Microsoft 365 Service

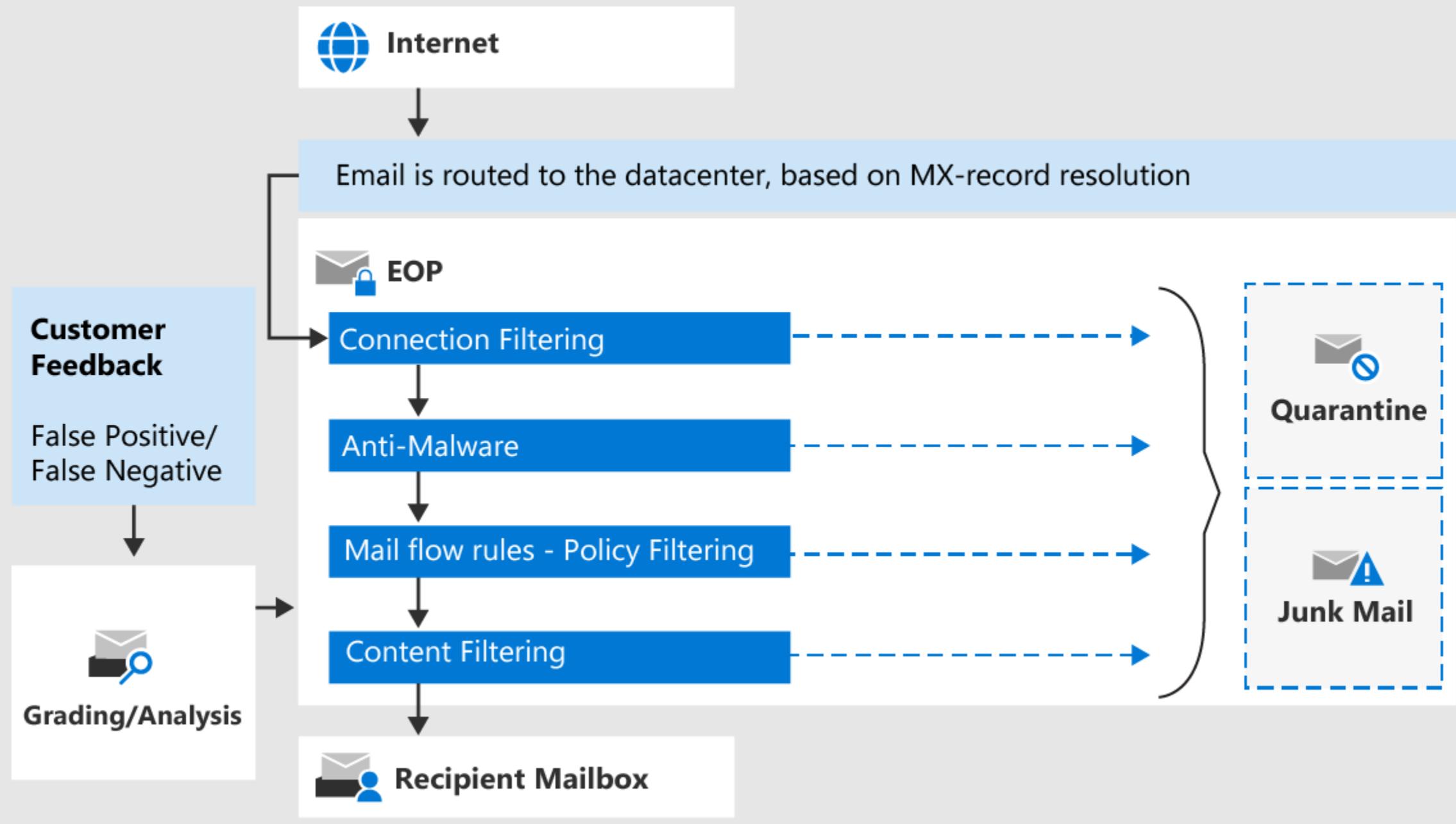
Email





Exercise: Enable Email authentication (SPF, DKIM, and DMARC)

DEMO



ORDER	EMAIL PROTECTION	CATEGORY	WHERE TO MANAGE
1	Malware	CAT:MALW	Configure anti-malware policies in EOP
2	High confidence phishing	CAT:HPHSH	Configure anti-spam policies in EOP
3	Phishing	CAT:PHSH	Configure anti-spam policies in EOP
4	High confidence spam	CAT:HSPM	Configure anti-spam policies in EOP
5	Spoofing	CAT:SPOOF	Spoof intelligence insight in EOP
6*	User impersonation (protected users)	CAT:UIMP	Configure anti-phishing policies in Microsoft Defender for Office 365
7*	Domain impersonation (protected domains)	CAT:DIMP	Configure anti-phishing policies in Microsoft Defender for Office 365
8*	Mailbox intelligence (contact graph)	CAT:GIMP	Configure anti-phishing policies in Microsoft Defender for Office 365
9	Spam	CAT:SPM	Configure anti-spam policies in EOP
10	Bulk	CAT:BULK	Configure anti-spam policies in EOP



Connection filter policy (Default)

- Always on | Priority Lowest

Always allow messages from the following IP addresses or address range:

Always block messages from the following IP addresses or address range:

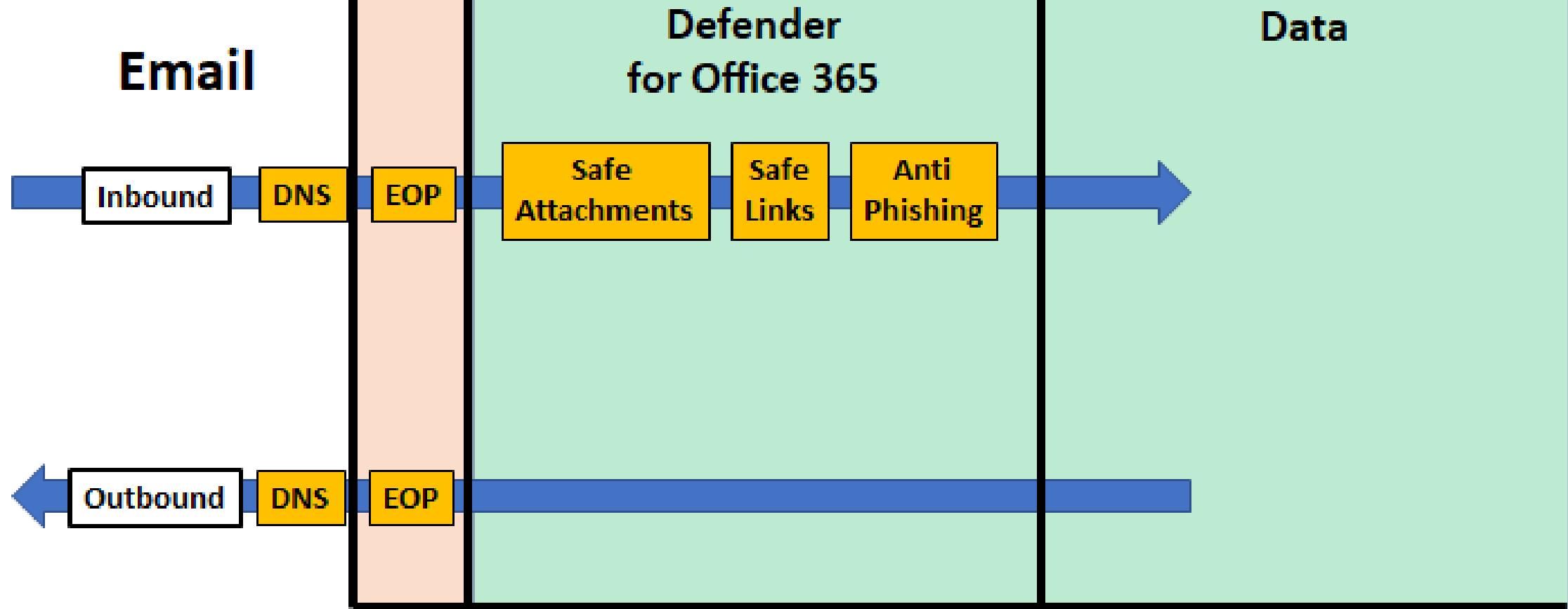
Turn on safe list

Safe list: The safe list in the connection filter policy is a dynamic allow list that requires no customer configuration. Microsoft identifies these trusted email sources from subscriptions to various third-party lists. You enable or disable the use of the safe list; you can't configure the servers in the list. Spam filtering is skipped on incoming messages from the email servers on the safe list.

Important points to note

- Protection stops for a recipient after the first policy is applied (the highest priority policy for that recipient).
- Multiple different types of conditions or exceptions are not additive; they're inclusive. The policy is applied only to those recipients that match all of the specified recipient filters.
- User impersonation protection does not work if the sender and recipient have previously communicated via email. If the sender and recipient have never communicated via email, the message can be identified as an impersonation attempt.
- Mailbox intelligence protection does not work if the sender and recipient have previously communicated via email. If the sender and recipient have never communicated via email, the message can be identified as an impersonation attempt by mailbox intelligence.

Microsoft 365



User configurable

The basics



Defender for Office 365

Analyzes email & files for anything suspicious

Safe Attachments

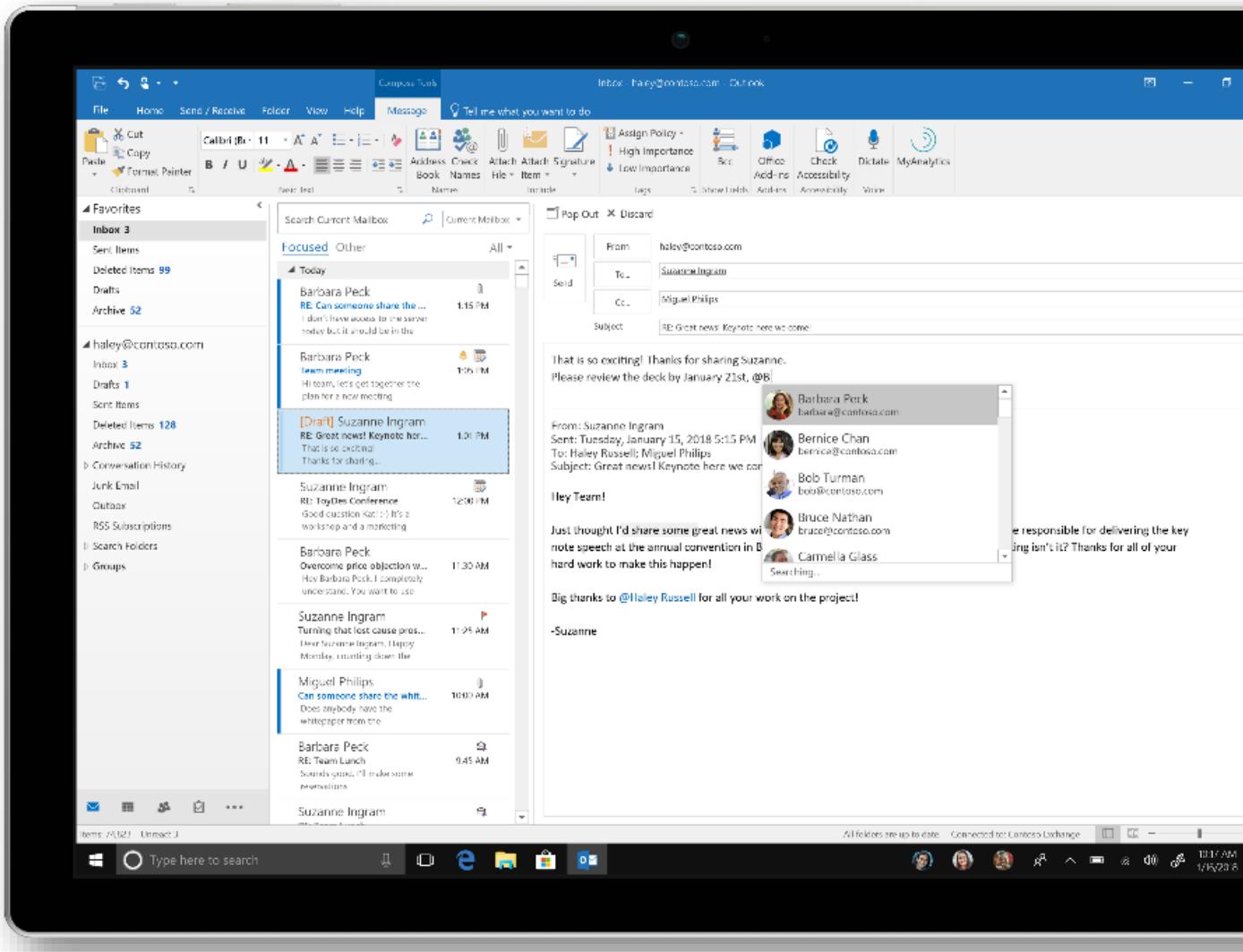
Set policies to **identify if email attachments are malicious**

Catch identified threats in corporate mail before they reach the inbox

Extend protection to files in SharePoint Online, OneDrive for Business, and Microsoft Teams

View ATP reports in the Office 365 Security and Compliance Center dashboard

How it works: Email attachments are opened and tested in a virtual environment. If malicious, the attachment is blocked. Protection also applies to attachments shared via SharePoint Online, OneDrive or Teams.

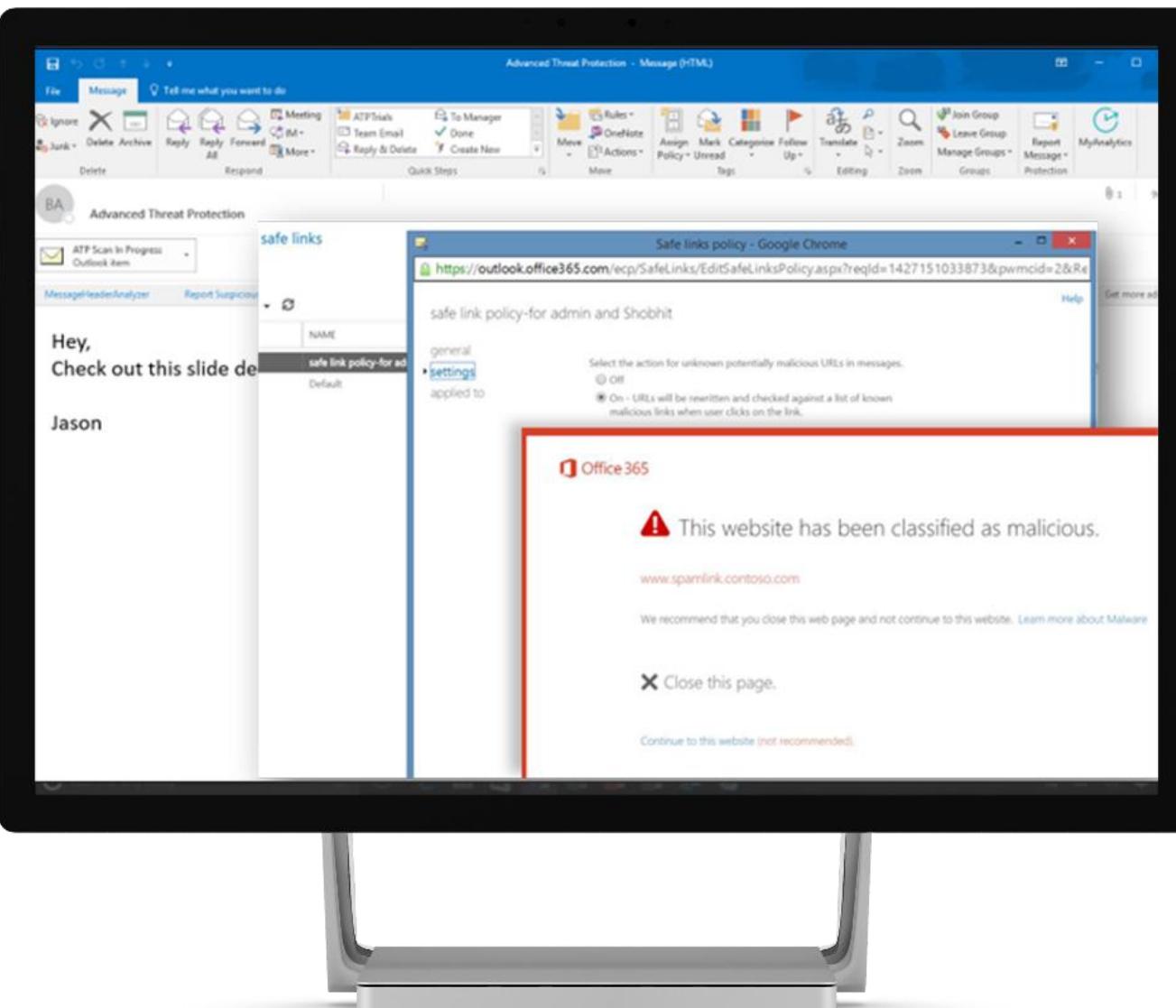


Safe Links & URL Detonation

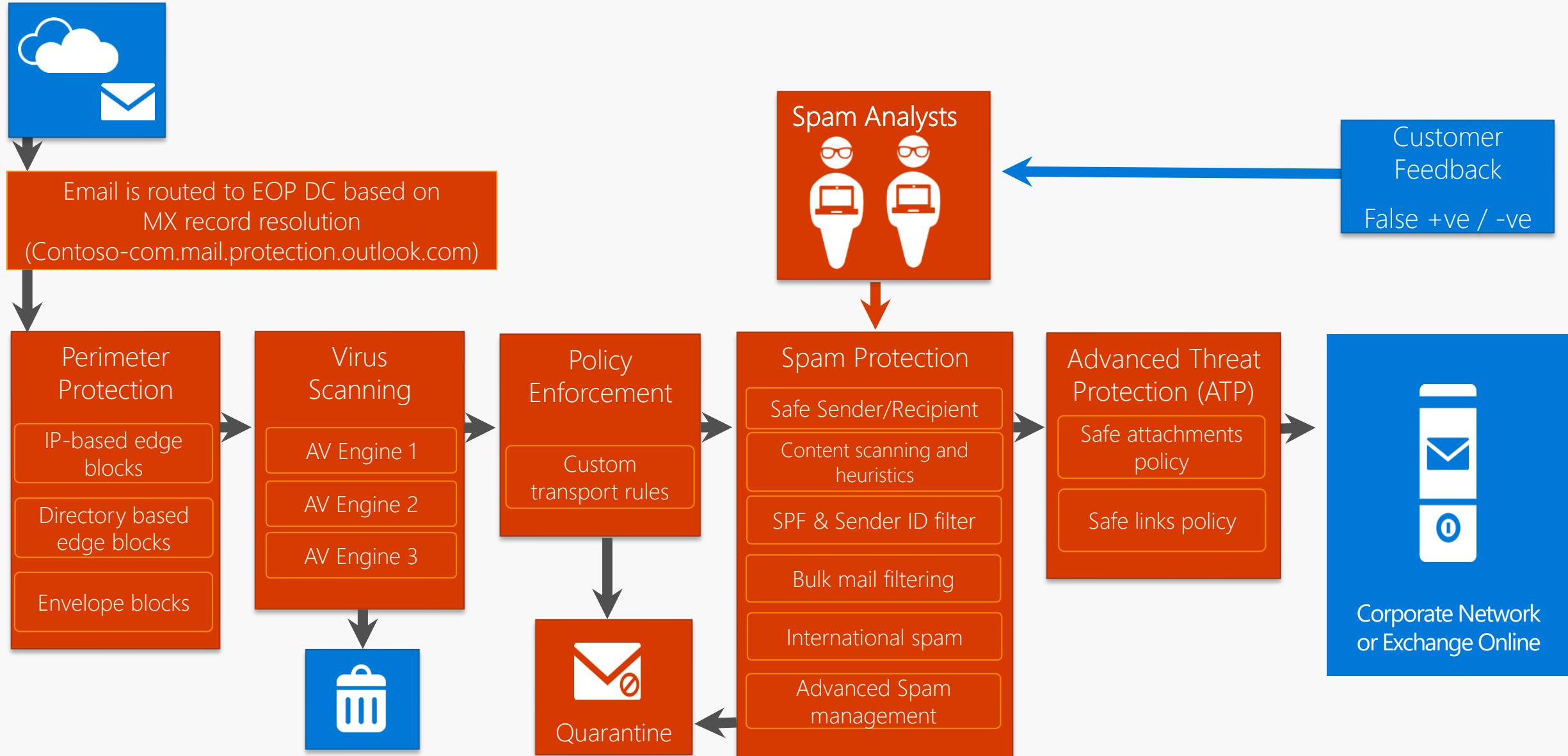
Prevent users from being compromised by files linked to malicious URLs

Safe Links policy can allow users to bypass warnings and enable tracing

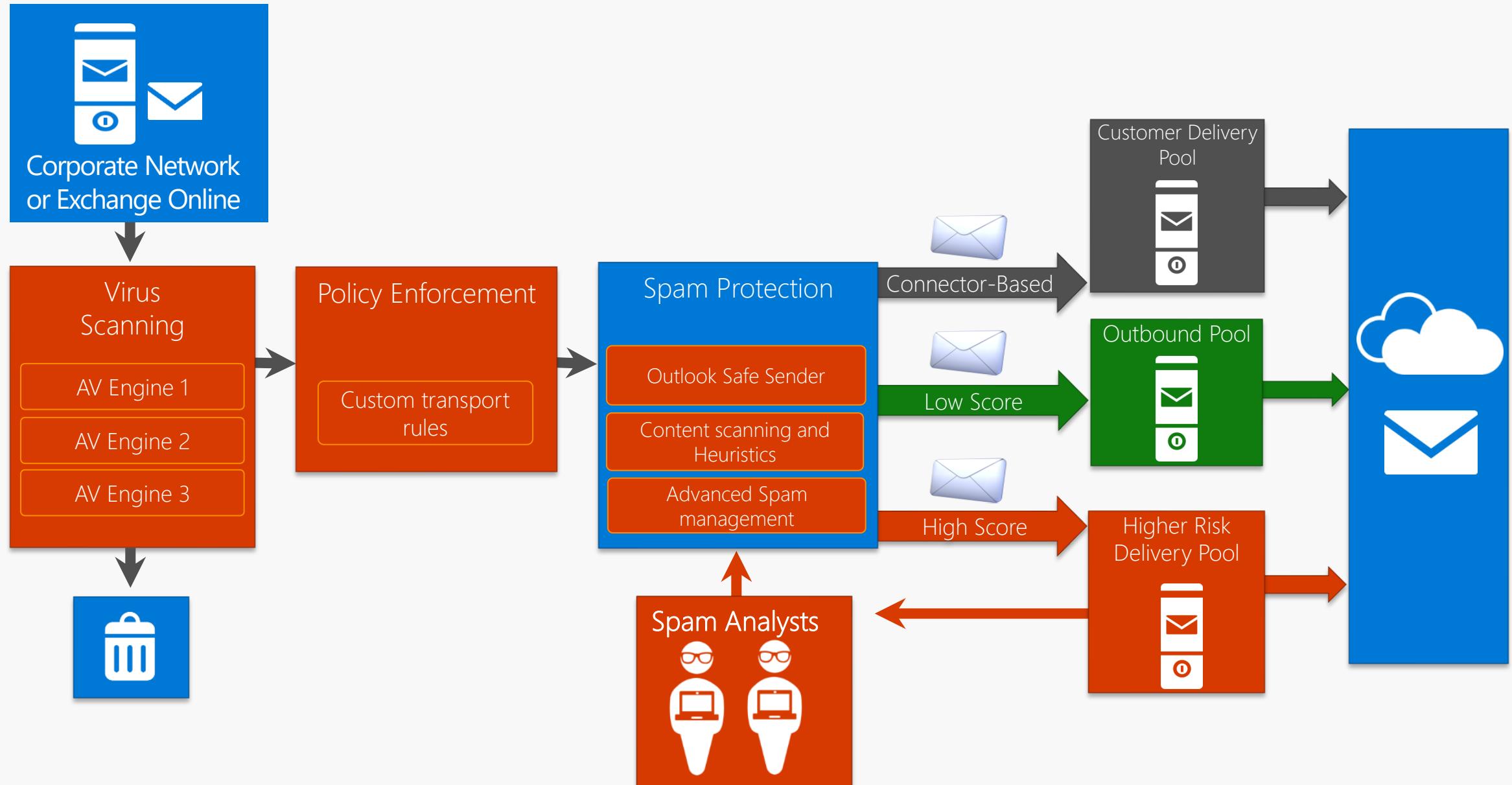
How it works :Each time a user clicks on a URL, the link is checked by ATP Safe Links before redirecting to the website.



Inbound Filtering

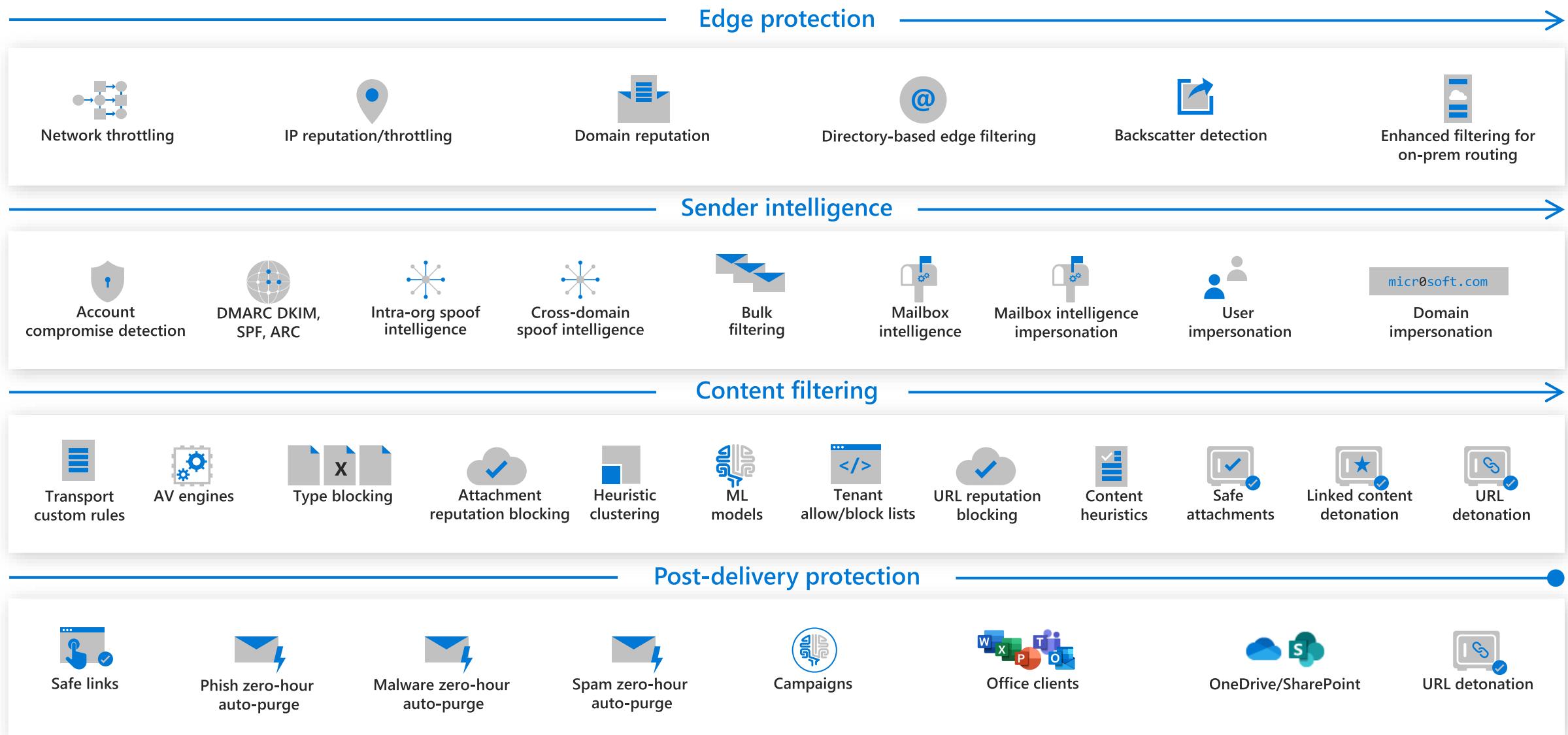


Outbound Filtering



Demo

Multi-Layered protection stack

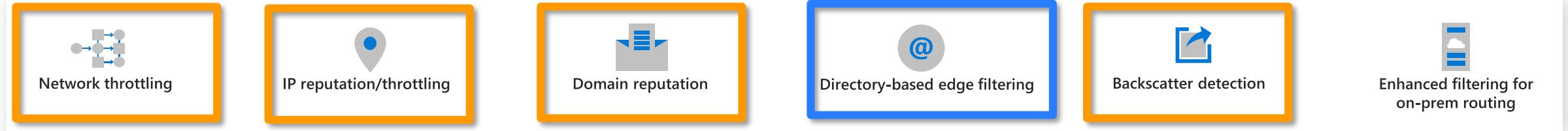


Multi-Layered protection stack

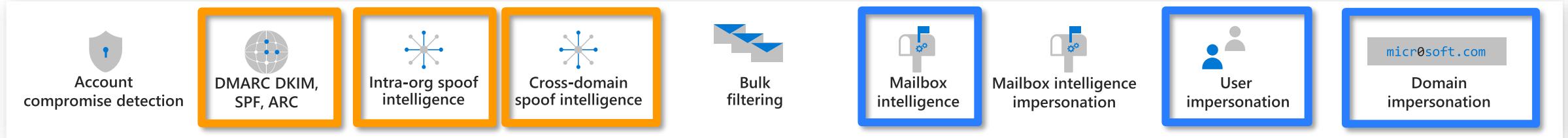
- Requires real sender as part of real mail flow

- Requires a real recipient with real mailboxes who actually interact with mails

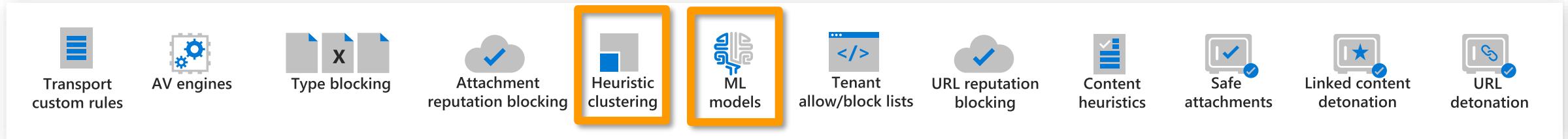
Edge protection



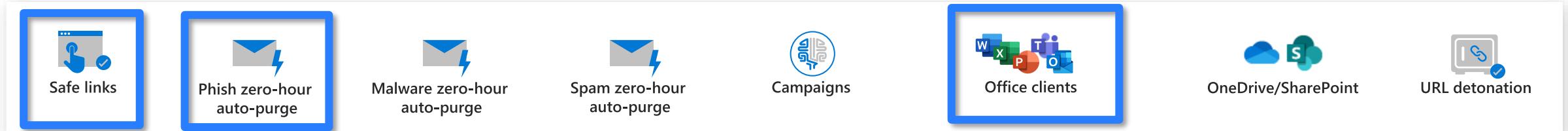
Sender intelligence



Content filtering



Post-delivery protection



Home Policies & rules > Threat policies

Threat policies

Templated policies

- Preset Security Policies Easily configure protection by applying all policies at once using our recommended protection.
- Configuration analyzer Identify issues in your current policy configuration to improve your security.

Policies

- Anti-phishing Protect users from phishing attacks, and configure safety tips on suspicious messages.
- Anti-spam Protect your organization's email from spam, including what actions to take if spam is detected.
- Anti-malware Protect your organization's email from malware, including what actions to take and who to notify.
- Safe Attachments Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Microsoft Teams.
- Safe Links Protect your users from opening and sharing malicious links in email messages and Office apps.

Rules

- Tenant Allow/Block Lists Manage allow or block entries for your organization.
- DKIM Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that emails are from your organization.
- Advanced delivery Manage overrides for special system use cases.
- Enhanced filtering Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record points to another provider.

Others

- User reported message settings Enable end users to report spam and malicious email for review and analysis.
- Evaluation mode Configure Microsoft Defender for Office 365 without impacting your production environment.

<https://security.microsoft.com/threatpolicy>

Preset security policies

A preset security policy is a compilation of settings for these security policies: anti-spam, anti-malware, anti-phishing, Safe Links, and Safe Attachments.

When multiple security policies are applied a user, the Strict policy overrides the Standard policy and any custom policies. The Standard policy overrides custom policies. [Learn more.](#)

Standard protection

Apply a baseline protection profile that's suitable for most users.



Disabled

Edit



Refresh

Exchange Online Protection applies to

Defender for Office 365 protections applies to

Strict protection

Apply a more aggressive protection profile for selected users.



Disabled

Edit



Refresh

Exchange Online Protection applies to

Defender for Office 365 protections applies to

Configuration analyzer

The configuration analyzer can help identify issues in your current configuration, and help improve your policies for better security. [Learn more.](#)

[Setting and recommendations](#)
[Configuration drift analysis and history](#)
[View Strict recommendations](#)
14 Standard recommendations


Search



Refresh

> Policy group/setting name	Policy	Applied to
> Anti-spam ■ All settings follow Standard recommendations		
▽ Anti-phishing ■ 10 recommendations		
Add users to protect	Office365 AntiPhish ...	
Include custom domains	Office365 AntiPhish ...	
If email is sent by an impersonated user	Office365 AntiPhish ...	
If email is sent by an impersonated domain	Office365 AntiPhish ...	
Show tip for impersonated users	Office365 AntiPhish ...	
If email is sent by an impersonated user who's prot...	Office365 AntiPhish ...	
Advanced phishing thresholds	Office365 AntiPhish ...	
If email is sent by someone who's not allowed to sp...	Office 365 ATP Anti ...	Included: 9 Domains;
Include custom domains	Office 365 ATP Anti ...	Included: 9 Domains;
If email is sent by an impersonated user	Office 365 ATP Anti ...	Included: 9 Domains;
> Anti-malware ■ 3 recommendations		
> Safe Attachments ■ 1 recommendations		
> Safe Links ■ All settings follow Standard recommendations		



<https://security.microsoft.com/configurationAnalyzer?viewid=Setting>

Demo

Stop auto-forwarding for email

The problem:

Hackers can access an email account and configure the mailbox to automatically forward to another email account, giving the hacker access to all info in these emails

The solution:

Turn off auto-forwarding for email; by creating a mail transport rule



Stop auto-forwarding for email

Stop auto-forwarding for email, by creating a mail transport rule:

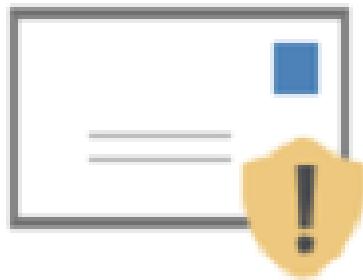
- In the Microsoft 365 admin center, click Admin centers > Exchange
- In the mail flow category, click rules
- Click +, and then click Create a new rule
- Click More options at the bottom of the dialog box to see the full set of options
- Apply the settings in the following table for each rule. Leave the rest of the settings at the default, unless you want to change these

Name	Prevent auto forwarding of email to external domains
Apply this rule if ...	The sender ... is external/internal ... Inside the organization
Add condition	The message properties ... include the message type ... Auto-forward
Do the following ...	Block the message ... reject the message and include an explanation
Provide message text	Auto-forwarding email outside this organization is prevented for security reasons

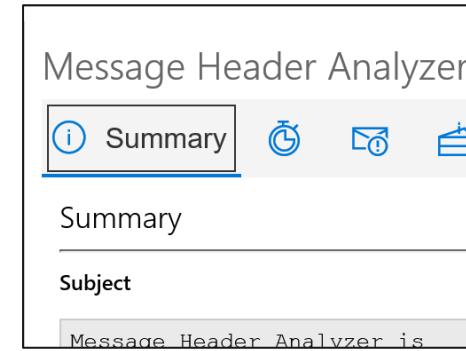
- Click Save

The screenshot shows two windows from the Microsoft 365 Admin Center. The top window is the 'Exchange admin center' rules list, showing a table with columns for ON, RULE, and PRIORITY. It lists three rules: 'Moderation for Lidia Holloway' (Priority 0), 'Signature for Lidia Holloway' (Priority 1), and 'Company Email Disclaimer' (Priority 2). The bottom window is a 'new rule' configuration dialog. The 'Name' field is 'Prevent auto forwarding of email to external domains'. The 'Apply this rule if...' section contains conditions: 'The sender is located... Inside the organization' and 'The message type is... Auto-forward'. The 'Do the following...' section contains an action: 'Reject the message with the explanation...'. A note in this section states: 'Auto-forwarding outside this organization is prevented for security reasons.' At the bottom right of the dialog are 'Save' and 'Cancel' buttons.

Outlook Add Ins



Report Message



Message Header Analyzer

Shared Mailboxes



Info

Sign-in blocked

[Reset password](#)

[Unblock sign-in](#)

[Delete user](#)



[Account](#)

[Devices](#)

[Licenses and apps](#)

[Mail](#)

[OneDrive](#)

Username

info@ciaops365.com

[Manage username](#)

Last sign-in

No attempts in last 30 days

[View last 30 days](#)

Alternate email address

None provided

[Add address](#)

Groups

[Manage groups](#)

Roles

No administrator access

[Manage roles](#)

Manage settings for email apps

Outlook on the web



Disabled

Outlook desktop (MAPI)



Disabled

Exchange web services



Disabled

Mobile (Exchange ActiveSync)



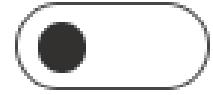
Disabled

IMAP



Disabled

POP

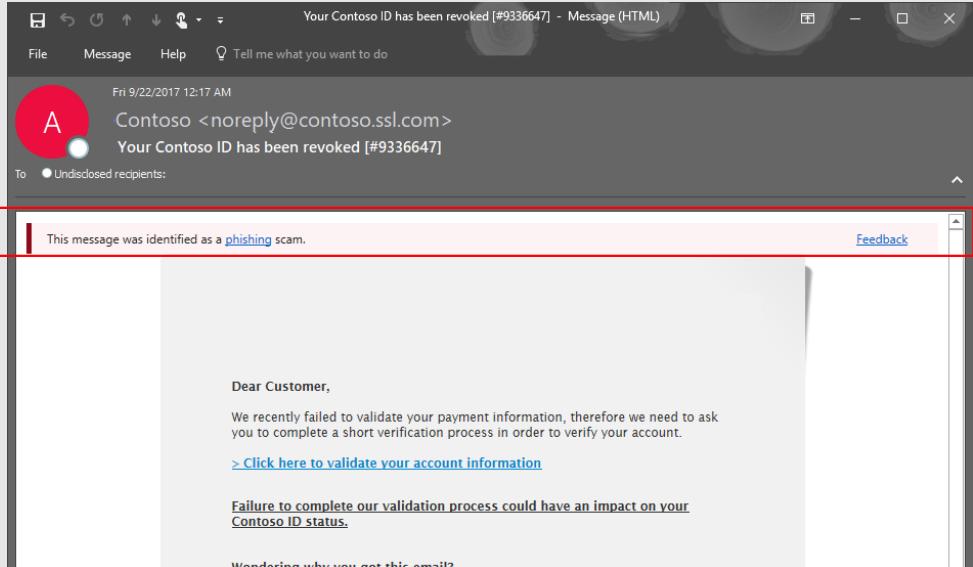


Disabled

User sign-ins (interactive)	User sign-ins (non-interactive)	Service principal sign-ins	Managed identity sign-ins			
Date	↑↓ Request ID	User	↑↓ Application	↑↓ Status	IP address	Location
2/16/2021, 6:29:59 PM	b457a5dd-ed07-490...	Info	Office 365 Exchange ...	Failure	178.33.132.48	AE

Details						
Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only	Additional Details
Date		2/16/2021, 6:29:59 PM	User	Info	Token issuer type	Azure AD
Request ID		b457a5dd-ed07-4909-98fa-1502dae64900	Username	info@ciaops365.com	Token issuer name	
Correlation ID		29933229-e2fc-4f2c-a24a-c2790b0a0b0a	User ID	db9d0850-fe7c-4d5c-bba6-e6e746af5992	Latency	237ms
Authentication requirement		Single-factor authentication	Alternate sign-in name	info@ciaops365.com	User agent	BAV2ROPC
Status	Failure		Application	Office 365 Exchange Online		
Sign-in error code	50053		Application ID	00000002-0000-0ff1-ce00-000000000000		
Failure reason	Other.		Resource	Office 365 Exchange Online		
			Resource ID	00000002-0000-0ff1-ce00-000000000000		
			Resource tenant ID	5243d63d-7632-4d07-a77e-de0fea1b77a4		
			Client app	IMAP4		

Intelligent Client Tips & Warnings for Suspicious Mails



Complete your survey New*

HR <HR@fabrikam.com>

Today, 3:28 PM
Philip Newman

You don't often get email from HR@FABRIKAMHR.COM, which appears similar to someone who has previously sent you email, but may not be that person. [Learn why this may be a problem](#)

This is a reminder that we are conducting a brief survey as part of Fabrikam's listening system, to provide feedback to our senior leaders, and you have been randomly selected to participate. The information from the survey helps leaders understand issues important to employees throughout the year.

The survey will remain open until Friday, September 29 at 6:00 p.m. Pacific Time. The survey should take less than 10 minutes to complete and the first 100 users will receive a \$50 dining card.

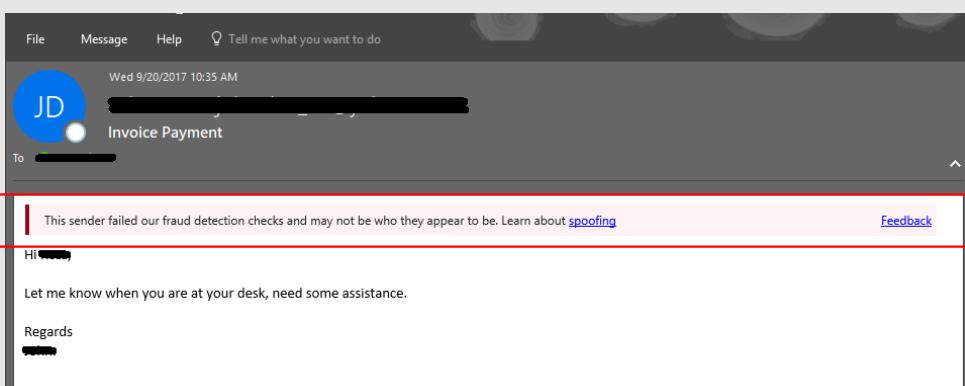
Follow this link to the Survey:
<http://fabrikam.com/survey/>

The Survey FAQ and privacy statement can be found at:
<http://fabrikam.com/survey/faq>

If you have any questions not answered in the FAQ, please contact esurvey@fabrikam.com.

Note: This link authenticates your Fabrikam credentials and takes you to an externally hosted survey. The authentication ensures secure data transfer as well as enables accurate reporting of results.

2017 Fabrikam. All rights reserved



Select Technique Name Simulation Select Payload Target Users Assign Training Launch Details Review Simulation

Select Technique

Select the social engineering technique you want to use with this simulation. We've curated these from the MITRE Attack framework. Depending on your selection, you will be able to use certain types of payloads.

Credential Harvest

In this type of technique, a malicious actor creates a message, with a URL in the message. When the target clicks on the URL within the message, they are taken to a web site, the website often...

[View details of credential harvest](#)

Malware Attachment

In this type of technique, a malicious actor creates a message, with an attachment added to the message. When the target opens the attachment, typically some arbitrary code such as a macro...

[View details of malware attachment](#)

Link in Attachment

In this type of technique, which is a hybrid of a Credential Harvest and Malware Attachment, a malicious actor creates a message, with a URL in an attachment, and then inserts the attachment into the message. When the target opens the attachment, they are represented with a URL in the actual attachment...

[View details of link in attachment](#)

Link to Malware

In this type of technique, a malicious actor creates a message, with an attachment added to the message. However instead of directly inserting the attachment into the message, the malicious actor will host the attachment on a well-known file sharing site, (such as SharePoint, or Dropbox) and insert the URL to the attachment file path...

[View details of link to malware](#)

Drive-by URL

In this type of technique, a malicious actor creates a message, with a URL in the message. When the target clicks on the URL within the message, they are taken to a website, the site will then try and run some background code to gather information about the target or deploy arbitrary code to their device...

[View details of Drive-by URL](#)

<https://security.microsoft.com/attacksimulator>

**Next****Save and close****Cancel**



- [Home](#)
- [Recipients](#)
- [Mailboxes](#)
- [Groups](#)
- [Resources](#)
- [Contacts](#)
- [Mail flow](#)
- [Roles](#)
- [Migration](#)
- [Mobile](#)
- [Reports](#)
- [Insights](#)
- [Public folders](#)
- [Organization](#)
- [Settings](#)
- [Other features](#)

- [Classic Exchange admin center](#)
- [Microsoft 365 admin center](#)

Mail flow reports

14 items

Name	Description
Auto forwarded messages report	Monitor for potential data leaks when people in your organization automatically forward email messages to an external domain, such as a personal email address.
Inbound messages report	Use this report to monitor message volume and TLS encryption for each connector. Mailflow between your Microsoft cloud organization, your on-premises email servers, and partner servers is often more important and you might want to apply extra security to these connections. Inbound includes messages from the internet and from on-premises organizations to Office 365.
Mail flow map report	View and learn the mail flow patterns to and from your Microsoft cloud organization, look for trends and anomalies, and fix issues.
Non-accepted domain report	This report shows messages from your on-premises organization where the sender's email domain isn't configured as an accepted domain in Office 365.
Non-delivery details report	Monitor messages that aren't getting delivered to the intended recipients. When a message can't be delivered, the sender gets an emailed non-delivery report (NDR) with an error code that indicates why the message wasn't delivered. This page shows the details of the NDRs and helps you troubleshoot the issues.
Outbound messages report	Use this report to monitor message volume and TLS encryption for each connector. Mailflow between your Microsoft cloud organization, your on-premises email servers, and partner servers is often more important and you might want to apply extra security to these connections. Outbound includes messages from Office 365 to the internet or to on-premises organizations.
SMTP AUTH clients report	Use this report to check for unusual activity and TLS used by clients or devices using SMTP AUTH. SMTP AUTH client submission protocol only offers basic authentication, which is often used by devices, such as printers,

Attack simulation training

Overview Simulations **Payloads** Simulation automations

Payloads are phishing emails and webpages that you use automatically with automations.

Draft Ready
0 120

Send a test Create a payload Copy payload

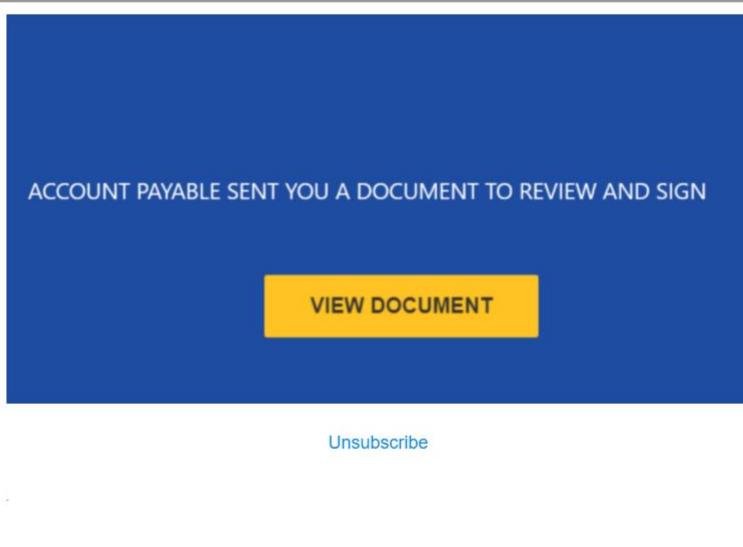
Payload name	Type	Source
2 Failed Messages	Social Engineering	Global
<input checked="" type="checkbox"/> Accounts payable docu...	Social Engineering	Global
American express pass...	Social Engineering	Global
American Express phon...	Social Engineering	Global
Applied Companies Inv...	Social Engineering	Global
Approval for Line of Cre...	Social Engineering	Global
Approval Requested:No...	Social Engineering	Global
Black Friday Offer	Social Engineering	Global
Blocked Facebook acco...	Social Engineering	Global
Capital One bank accou...	Social Engineering	Global
Claim a fax document	Social Engineering	Global

↑ ↓ ×

Accounts payable document review

Social Engineering • Credential Harvest

Overview Simulations launched



Unsubscribe

Payload Description

This payload looks like it comes from accounts payable, asking the user to review and sign a document.

From name Account Payable	From Email heather@heathercooper.co.uk
Email subject Account Payable Sent You A Document To Review And Sign]	Source Global

Demo

Edge protection



Network throttling



IP reputation/throttling



Domain reputation



Directory-based edge filtering



Backscatter detection

Sender intelligence



DMARC
DKIM,
SPF, ARC



Intra-org spoof
intelligence



Cross-domain
spoof intelligence



Bulk
filtering



Mailbox
intelligence



User
impersonation



Domain
impersonation

Content filtering



Transport
custom rules



AV engines



Type blocking



Attachment
reputation blocking



Heuristic
clustering



ML
models



URL reputation
blocking



Content
heuristics



Safe
attachments



Linked content
detonation



URL
detonation

Post-delivery protection



Linked content
detonation



Safe links



Zero-hour
auto-purge



Safe links for
Office clients

Edge protection



Network throttling



IP reputation/throttling



Domain reputation



Directory-based edge filtering



Backscatter detection



Network throttling protects Office 365 infrastructure and customers from Denial of Service attacks by limiting the number of messages that can be submitted by a specific set of infrastructure.

Edge protection



Network throttling



IP reputation/throttling



Domain reputation



Directory-based edge filtering



Backscatter detection



IP reputation and throttling will block messaging being sent from known bad connecting IP addresses. If a specific IP sends a large number of messages in a short period of time they will be throttled.

Edge protection



Network throttling



IP reputation/throttling



Domain reputation



Directory-based edge filtering

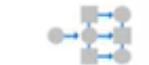


Backscatter detection



Domain reputation will block any messages at the edge being sent from a known bad domain.

Edge protection



Network throttling



IP reputation/throttling



Domain reputation



Directory-based edge filtering



Backscatter detection

Directory-based edge filtering blocks attempts to harvest an organizations directory information through SMTP.

Edge protection



Network throttling



IP reputation/throttling



Domain reputation



Directory-based edge filtering



Backscatter detection

Backscatter detection prevents an organization from being attacked through invalid NDRs.

Sender intelligence



DMARC
DKIM,
SPF, ARC



Intra-org spoof
intelligence



Cross-domain
spoof intelligence



Bulk
filtering



Mailbox
intelligence



User
impersonation



Domain
impersonation

Features within sender intelligence are critical for catching a great deal of spam, bulk, and unauthorized spoof and is an important factor in phish detection. Most of these features are individually configurable.



SPF enforces rejecting mails based on which IPs are allowed to send mail on the organizations behalf as define in their DNS record.

DKIM provides an encrypted signature that authenticates the sender.

DMARC allows the sender to mark their domain as requiring SPF and DKIM ensuring alignment between these two technologies.

Sender intelligence



DMARC
DKIM,
SPF, ARC



Intra-org
spoof
intelligence



Cross-domain
spoof intelligence



Bulk
filtering



Mailbox
intelligence

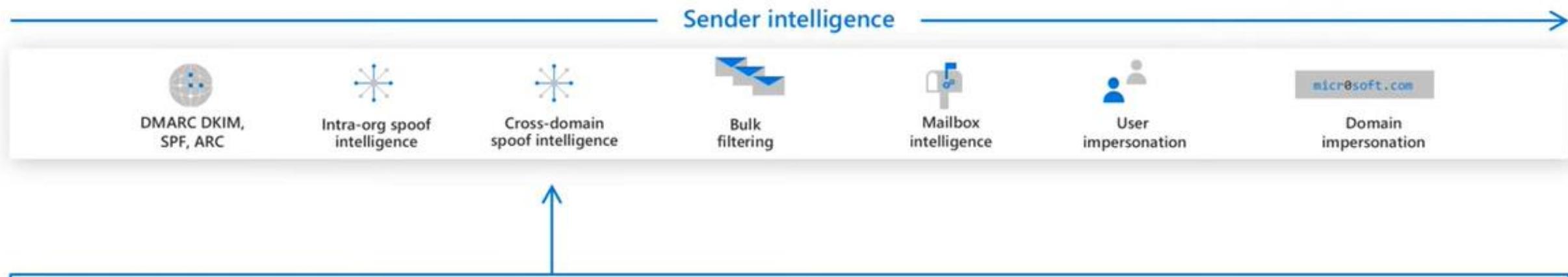


User
impersonation

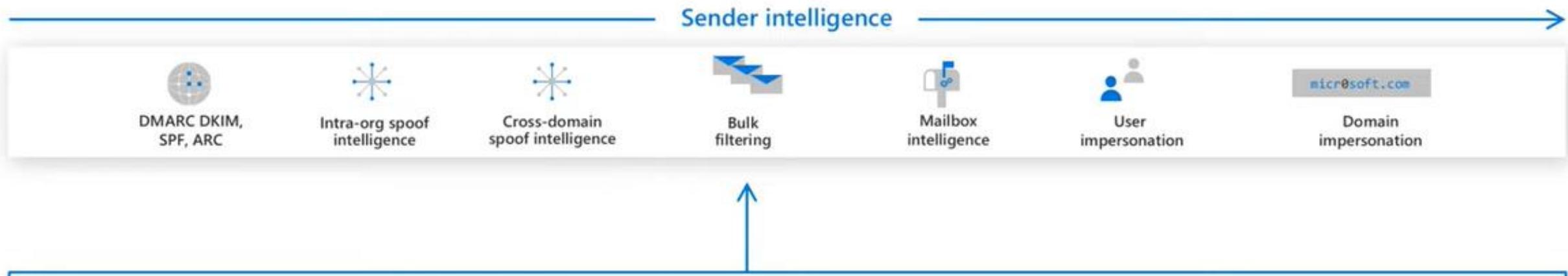


Domain
impersonation

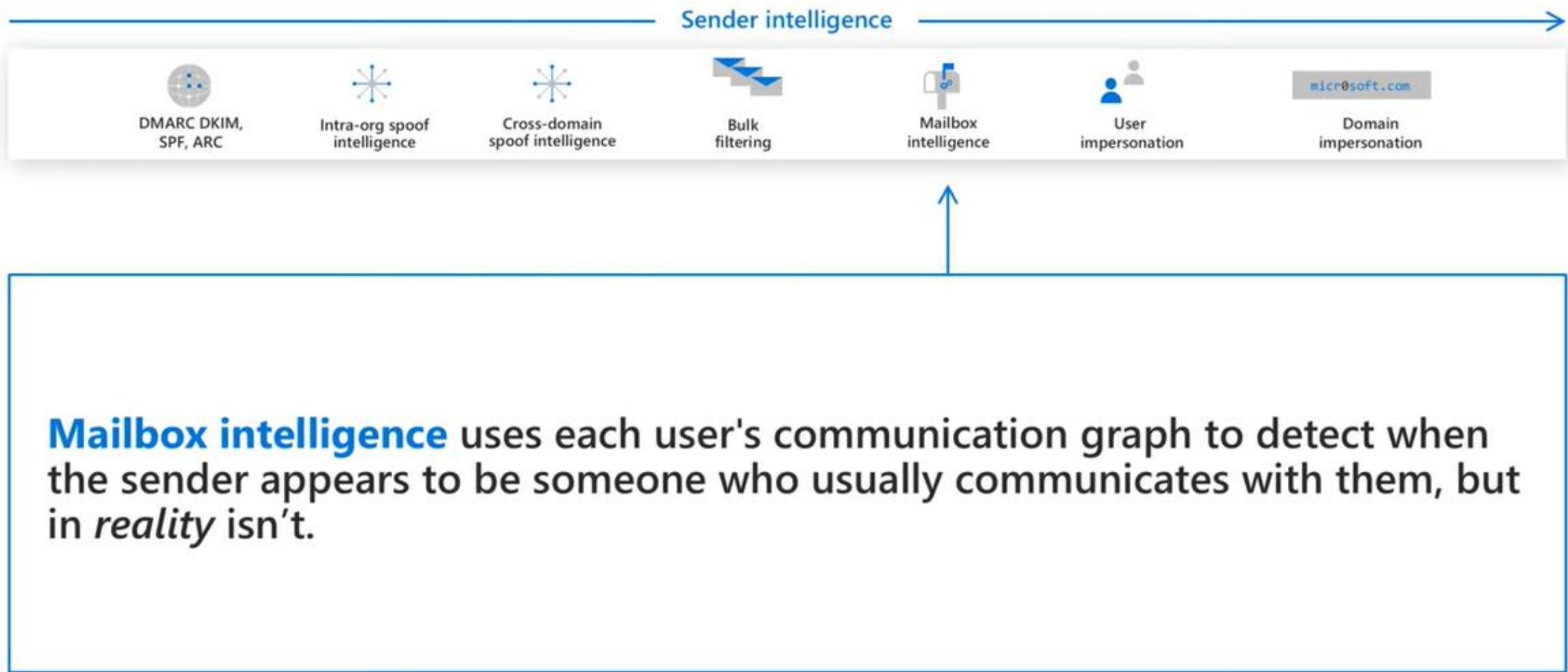
Intra-org spoof intelligence detects and blocks spoof attempt from a domain within the organization.

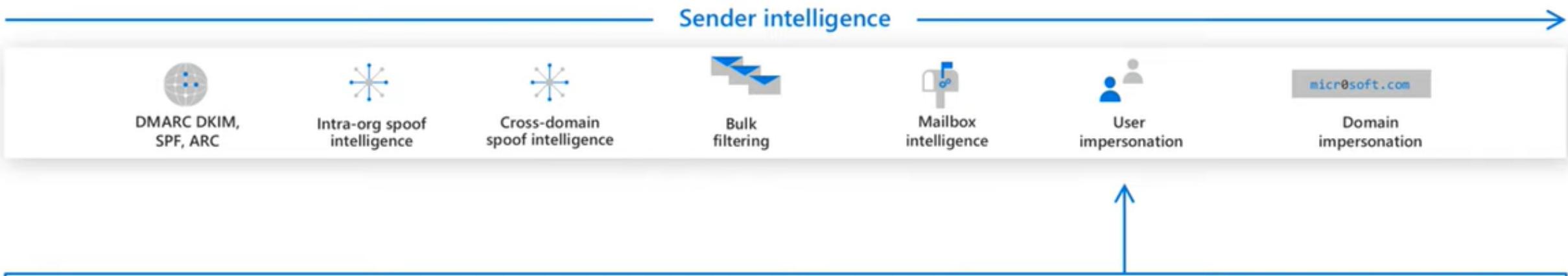


Cross-domain spoof intelligence detects and blocks spoof attempt from a domain outside of the organization.

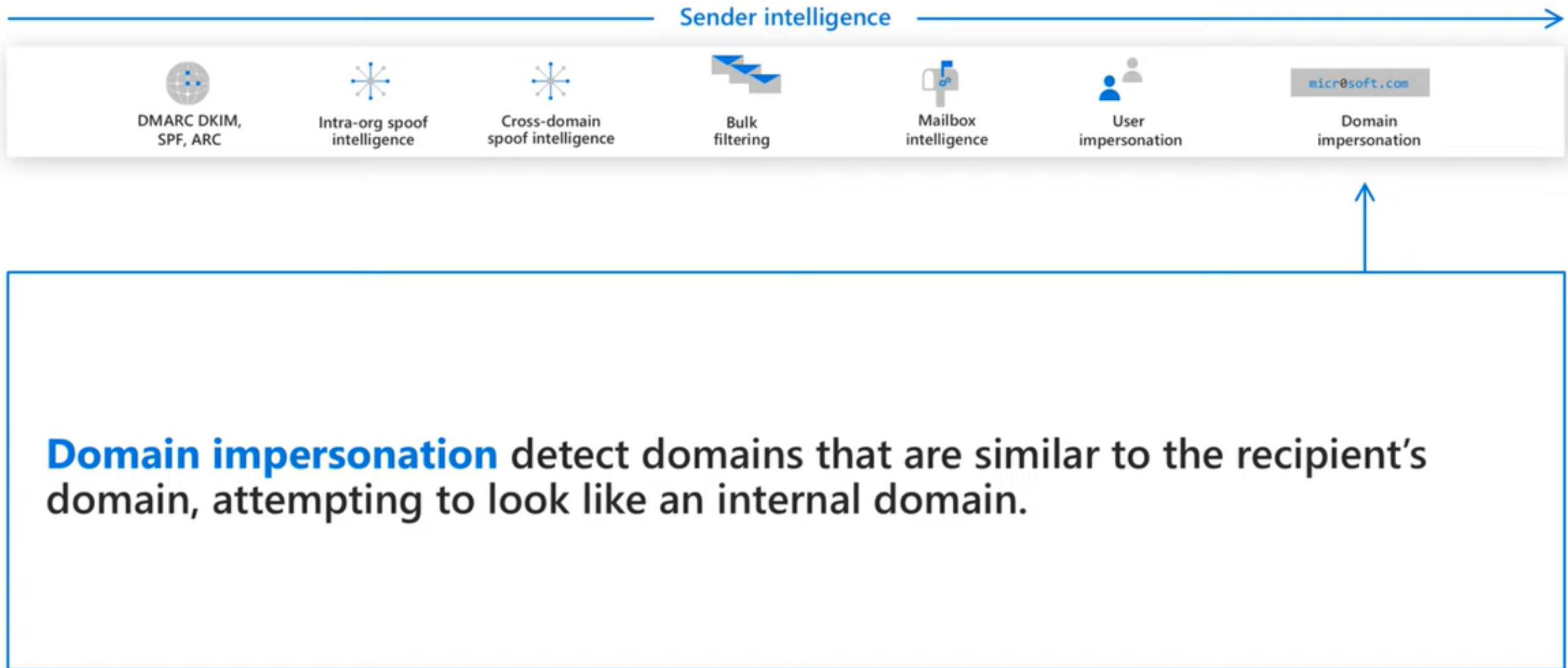


Bulk filtering provides a confidence level (BCL) indicating whether or not the message was sent from a bulk sender. Customers can use the Bulk Slider in the Antispam policy to decide what level of bulk to treat as spam.





User impersonation allows an admin to provide a list of high value targets that are likely to be impersonated within their organization. If a mail arrives with a sender with the same name, but a different address the recipient is warned.



Content filtering



Transport rules also known as ETRs, allow an admin to perform a wide range of complex action when an equally wide range of conditions are met for a given message.

Content filtering



MSAV and multiple **AV engines** are used to detect all known malware in attachments.

Content filtering



The AV engines are also used to true-type all attachments so that **type blocking** can block all attachment of the types the admin specifies.

Content filtering



Whenever ATP detects a malicious attachment the file's hash and a hash of its active content are added to EOP reputation. **Attachment reputation blocking** will then block that file across all of O365 and on endpoints through MSAV cloud calls.

Content filtering



Heuristic clustering can determine that a file is suspicious based on delivery heuristics. When a suspicious attachment is found the entire campaign is paused and the file is sandboxed. If it is found to be malicious the entire campaign is blocked.

Content filtering



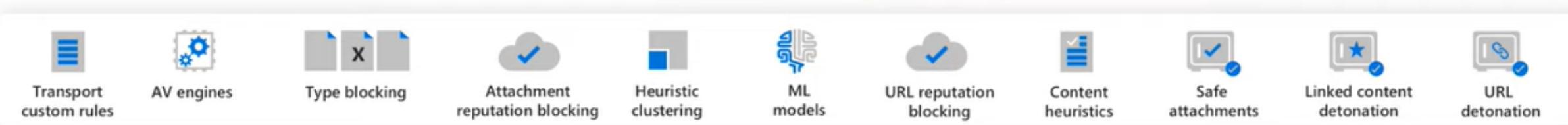
Machine learning models act on the header, body content, and URLs of a message to detect phishing attempts.

Content filtering



We use our own reputation from URL sandboxing as well as URL reputation from third party feeds in **URL reputation blocking** to block any message with a known malicious URL.

Content filtering



Content heuristics can detect suspicious messages based on structure and word frequency within the body of the message using machine learning models.

Content filtering



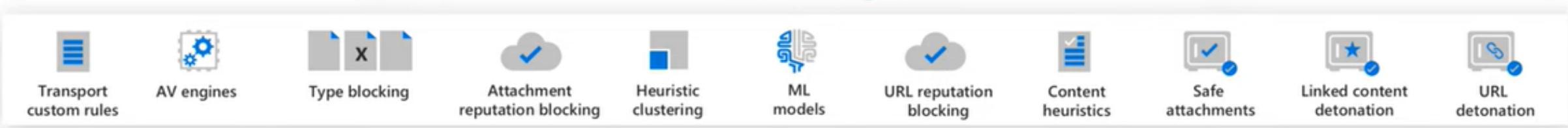
Safe attachments sandboxes every attachment for ATP customers, using dynamic analysis to detect never before seen threats.

Content filtering



Linked content detonation treats every URL linking to a file in an email as an attachment, asynchronously sandboxing the file at time of delivery.

Content filtering



When the upstream anti-phish tech finds a message or URL to be suspicious, **URL detonation** sandboxes the URLs in the message at time of delivery.

Post-delivery protection



Linked content
detonation



Safe links



Zero-hour
auto-purge



Safe links for
Office clients

When a URL that points to a file is clicked on post delivery, **linked content detonation** displays a warning page until sandboxing of the file is complete and the URL is found to be safe.

Post-delivery protection



Linked content
detonation



Safe links



Zero-hour
auto-purge



Safe links for
Office clients



Safe links is Office 365 ATP's time of click protection. Every URL in each message is wrapped to point to our Safe Links servers. When the URL is clicked it is checked against the latest reputation before the user is redirected to the target site and the URL is asynchronously sandboxed to update our reputation.

Post-delivery protection



Linked content
detonation



Safe links



Zero-hour
auto-purge



Safe links for
Office clients



Zero-hour auto-purge can find and junk any message with an attachment or a URL that is found to be malicious after the message has been delivered.

Post-delivery protection



Linked content
detonation



Safe links



Zero-hour
auto-purge



Safe links for
Office clients

Safe links for Office clients offers the same Safe links time of click protection natively inside of Office clients, like Word, PowerPoint, and Excel.

Edge protection



Network throttling



IP reputation/throttling



Domain reputation



Directory-based edge filtering



Backscatter detection

Sender intelligence



DMARC
DKIM,
SPF, ARC



Intra-org spoof
intelligence



Cross-domain
spoof intelligence



Bulk
filtering



Mailbox
intelligence



User
impersonation



Domain
impersonation

Content filtering



Transport
custom rules



AV engines



Type blocking



Attachment
reputation blocking



Heuristic
clustering



ML
models



URL reputation
blocking



Content
heuristics



Safe
attachments



Linked content
detonation



URL
detonation

Post-delivery protection



Linked content
detonation



Safe links



Zero-hour
auto-purge



Safe links for
Office clients