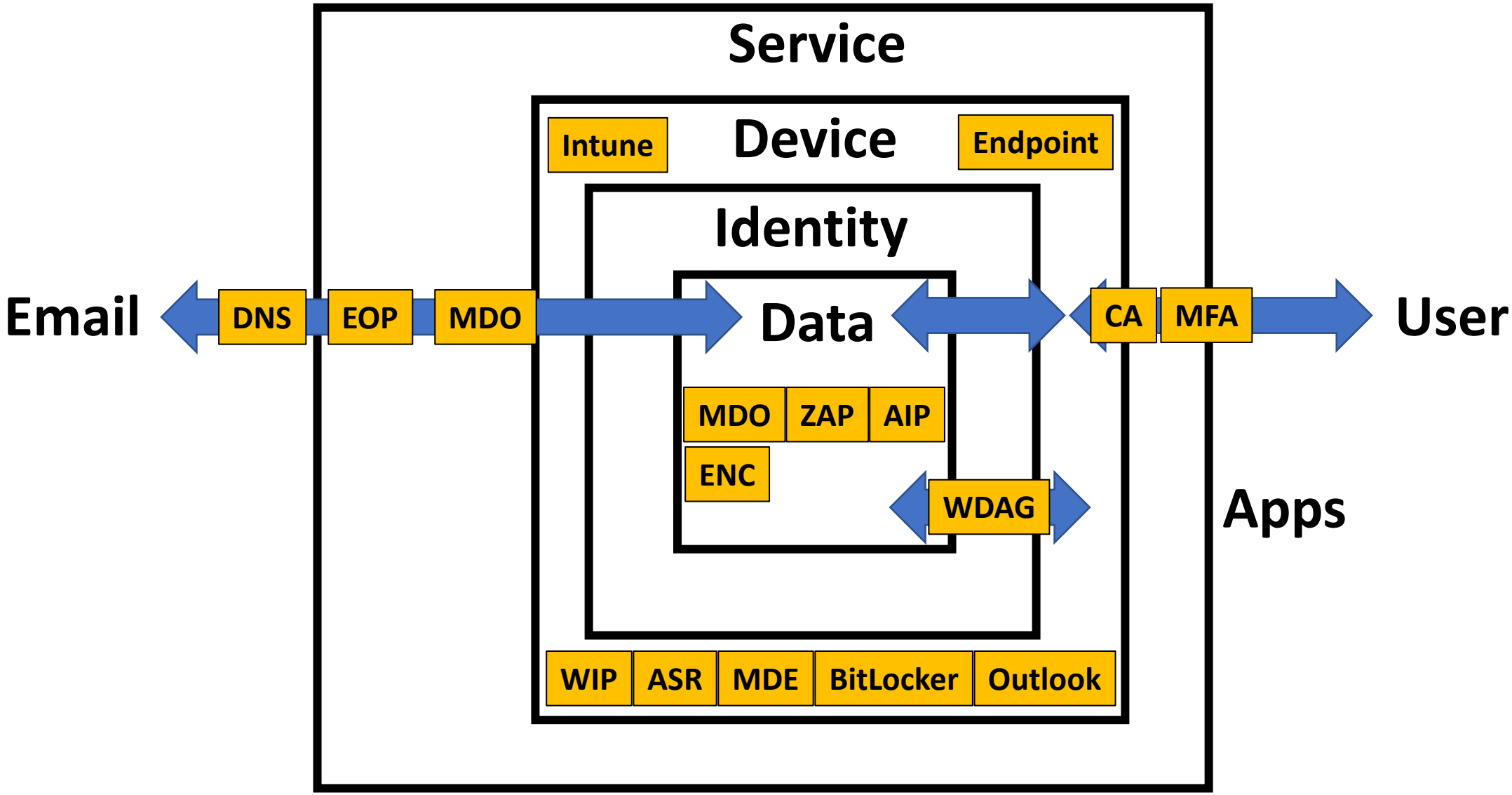
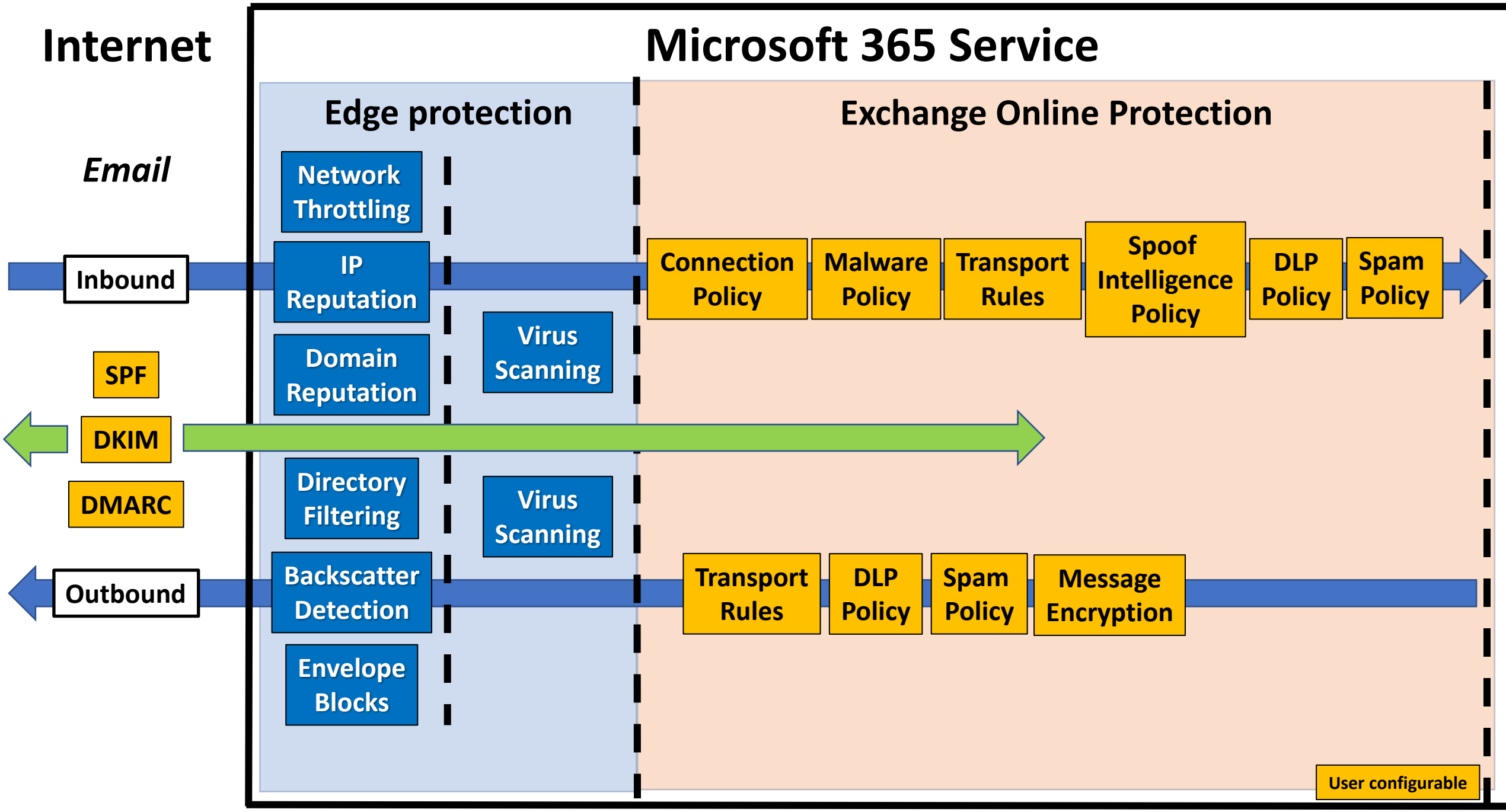
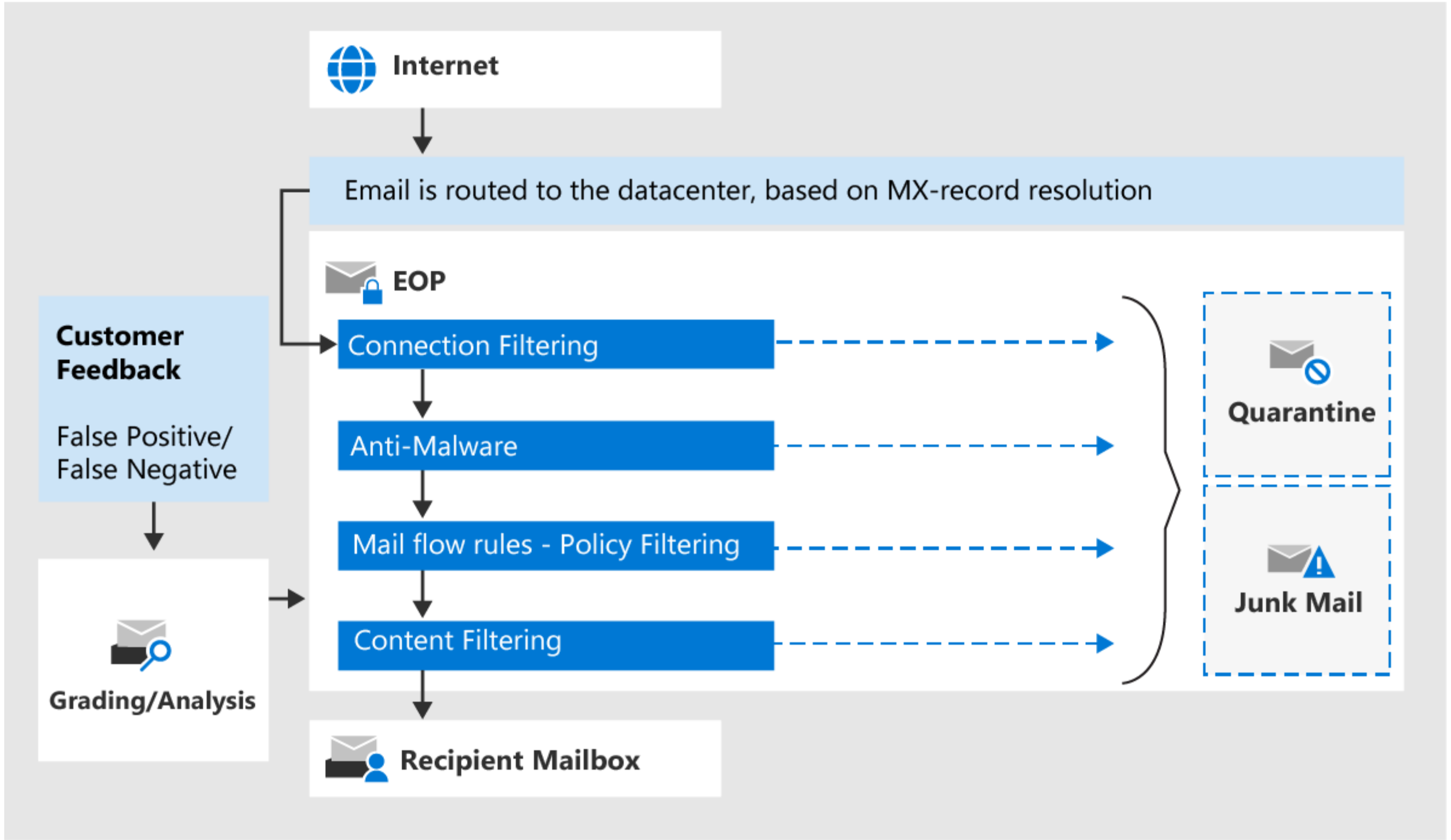
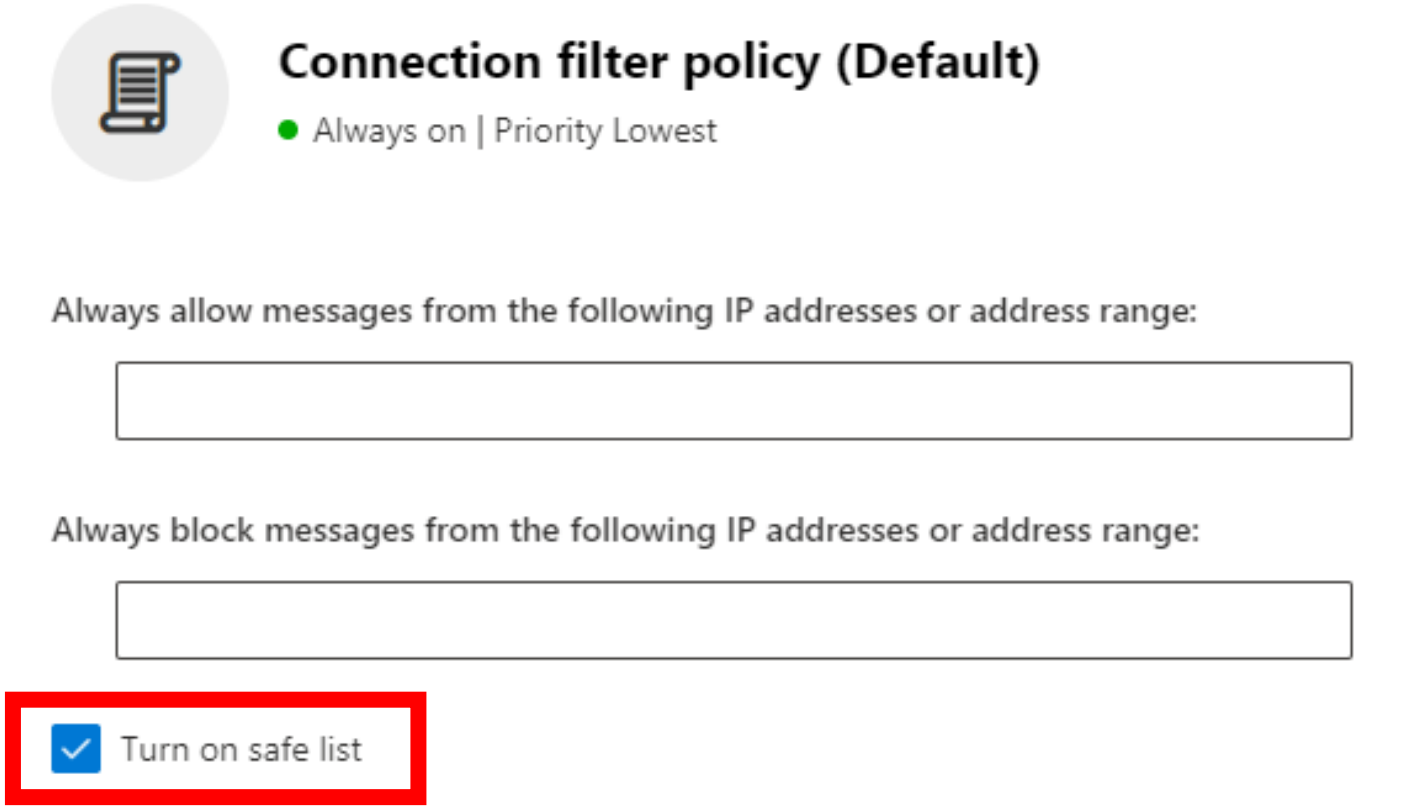
Email


Service
Device
Intune
Endpoint
Identity
Data
Email
DNS
EOP
MDO
CA
MFA
User
MDO
ZAP
AIP
ENC
WDAG
Apps
WIP
ASR
MDE
BitLocker
Outlook


Internet
Microsoft 365 Service
Edge protection
Exchange Online Protection
Email
Network Throttling
IP Reputation
Domain Reputation
Virus Scanning
Directory Filtering
Virus Scanning
Backscatter Detection
Envelope Blocks
Inbound
SPF
DKIM
DMARC
Outbound
Connection Policy
Malware Policy
Transport Rules
Spoof Intelligence Policy
DLP Policy
Spam Policy
Transport Rules
DLP Policy
Spam Policy
Message Encryption
User configurable


Internet
Email is routed to the datacenter, based on MX-record resolution
EOP
Customer Feedback
False Positive/
False Negative
Connection Filtering
Anti-Malware
Mail flow rules - Policy Filtering
Content Filtering
Quarantine
Junk Mail
Grading/Analysis
Recipient Mailbox



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.

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/connection-filter-policies-configure?view=o365-worldwide

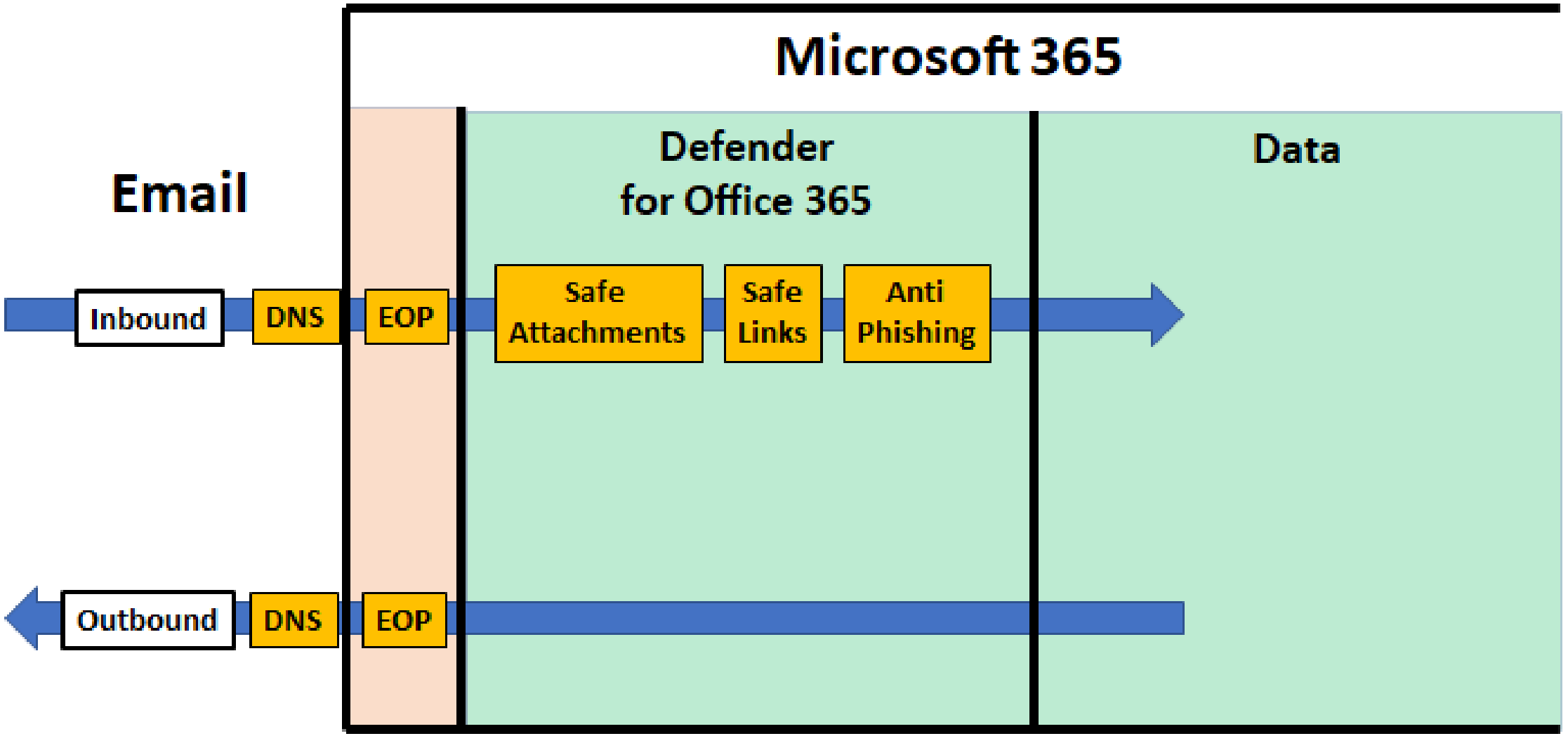
Order	Email protection	Category	Where to manage
1	Malware	CAT:MALW	Configure anti-malware policies in EOP
2	High confidence phishing	CAT:HPHSH	Configure anti-spam policies in EOP
3	Phishing	CAT:PHSH	Configure anti-spam policies in EOP
4	High confidence spam	CAT:HSPM	Configure anti-spam policies in EOP
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

* These features are available only in anti-phishing policies in Microsoft Defender for Office 365.

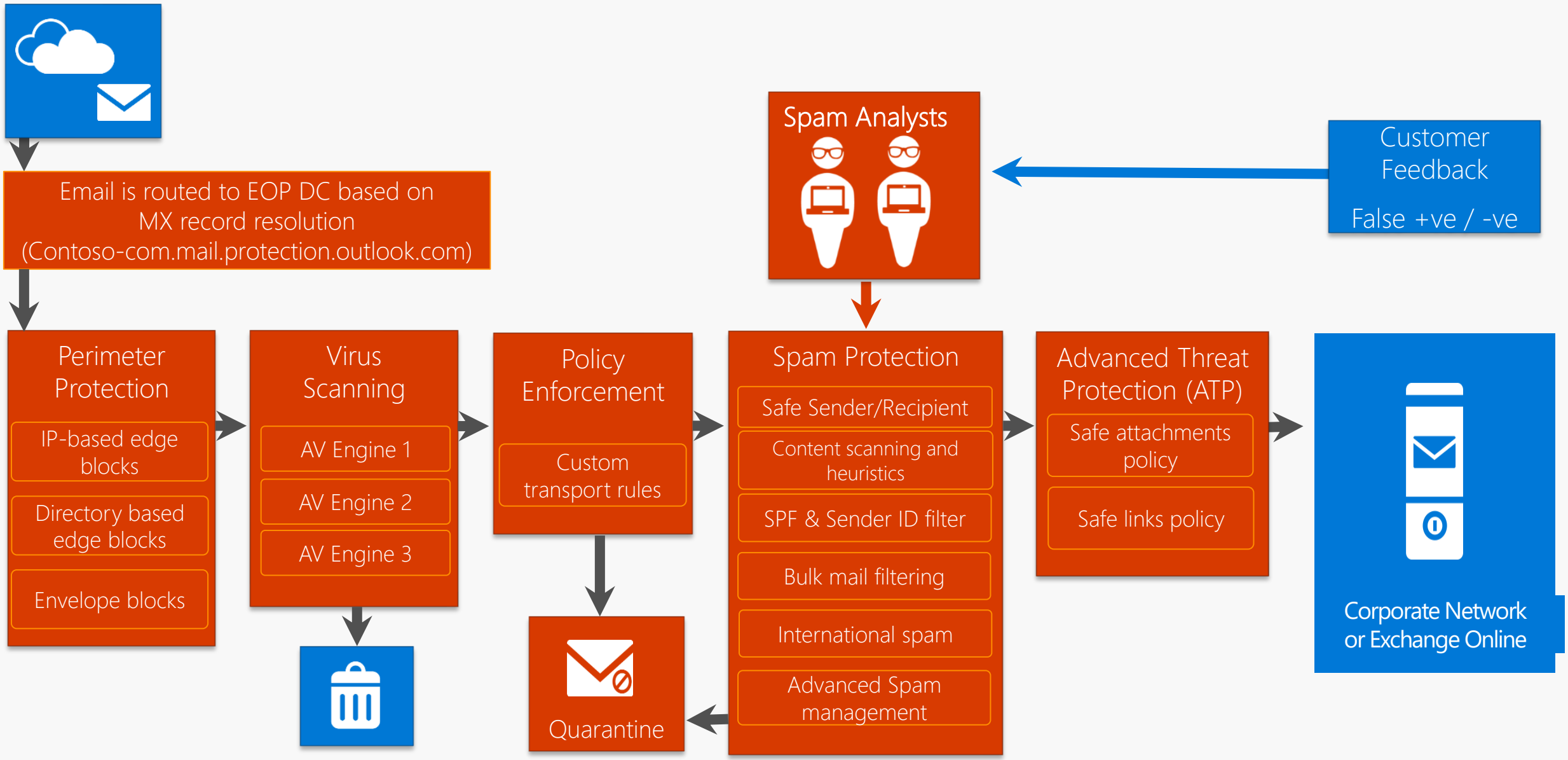
The priority order of policies: The policy priority order is shown in the following list:

1. The anti-spam, anti-malware, anti-phishing, Safe Links*, and Safe Attachments* policies in the Strict preset security policy (when enabled).
2. The anti-spam, anti-malware, anti-phishing, Safe Links*, and Safe Attachments* policies in the Standard preset security policy (when enabled).
3. Anti-phishing, Safe Links, and Safe Attachments in Defender for Office 365 evaluation policies (when enabled).
4. Custom anti-spam, anti-malware, anti-phishing, Safe Links*, and Safe Attachments* policies (when created).
5. Custom policies are assigned a default priority value when you create the policy (newer equals higher), but you can change the priority value at any time. This priority value affects the order that *custom policies* of that type (anti-spam, anti-malware, anti-phishing, etc.) are applied, but doesn't affect where custom policies are applied in the overall order.
6. Of equal value:
    1. The Safe Links and Safe Attachments policies in the Built-in protection preset security policy*.
    2. The default policies for anti-malware, anti-spam, and anti-phishing.
7. You can configure exceptions to the Built-in protection preset security policy, but you can't configure exceptions to the default policies (they apply to all recipients and you can't turn them off).

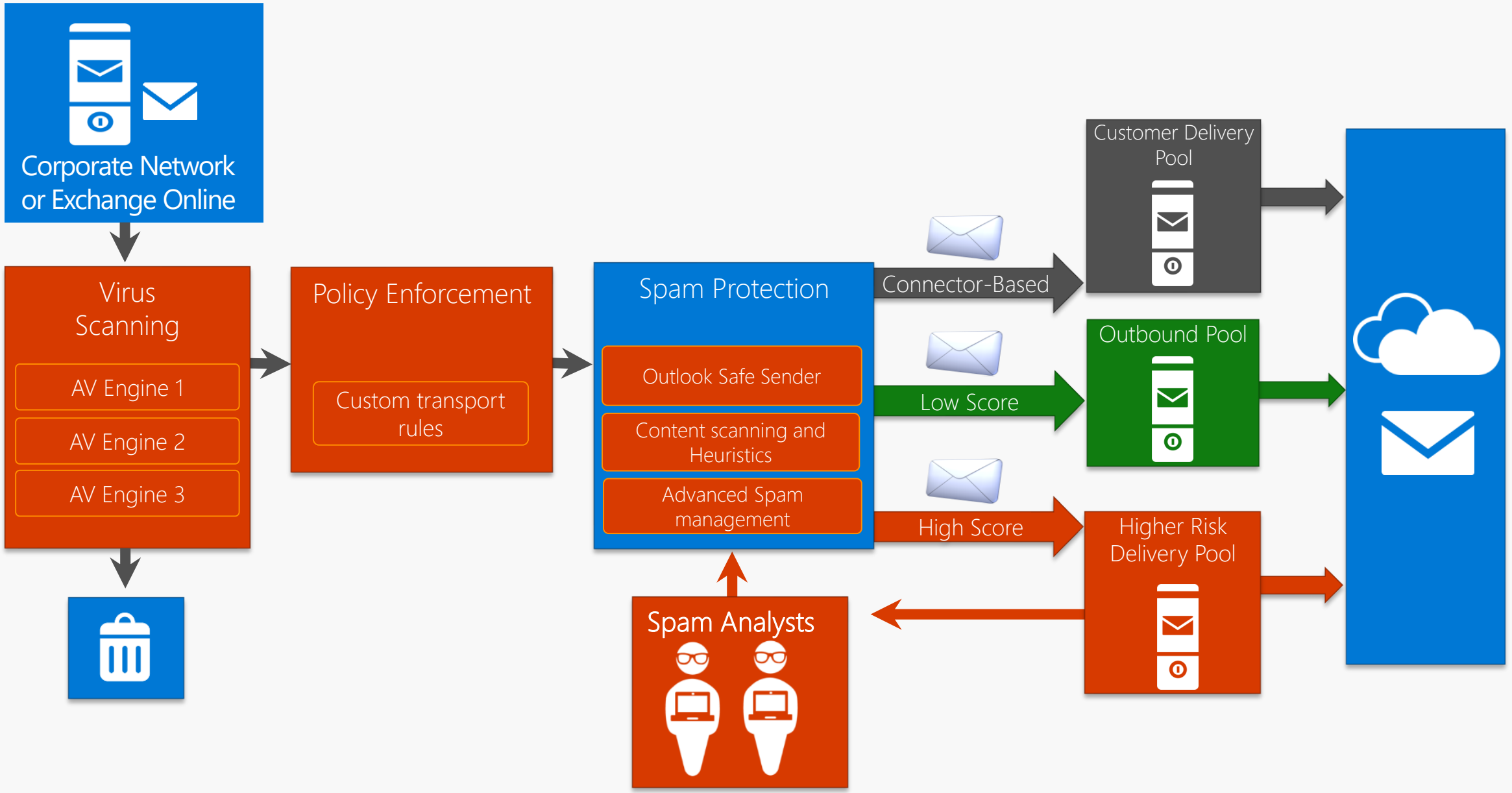
* Defender for Office 365 only.


Microsoft 365
Email
Defender
for Office 365
Data
Inbound
DNS
EOP
Safe
Attachments
Safe
Links
Anti
Phishing
Outbound
DNS
EOP
User configurable

Inbound Filtering

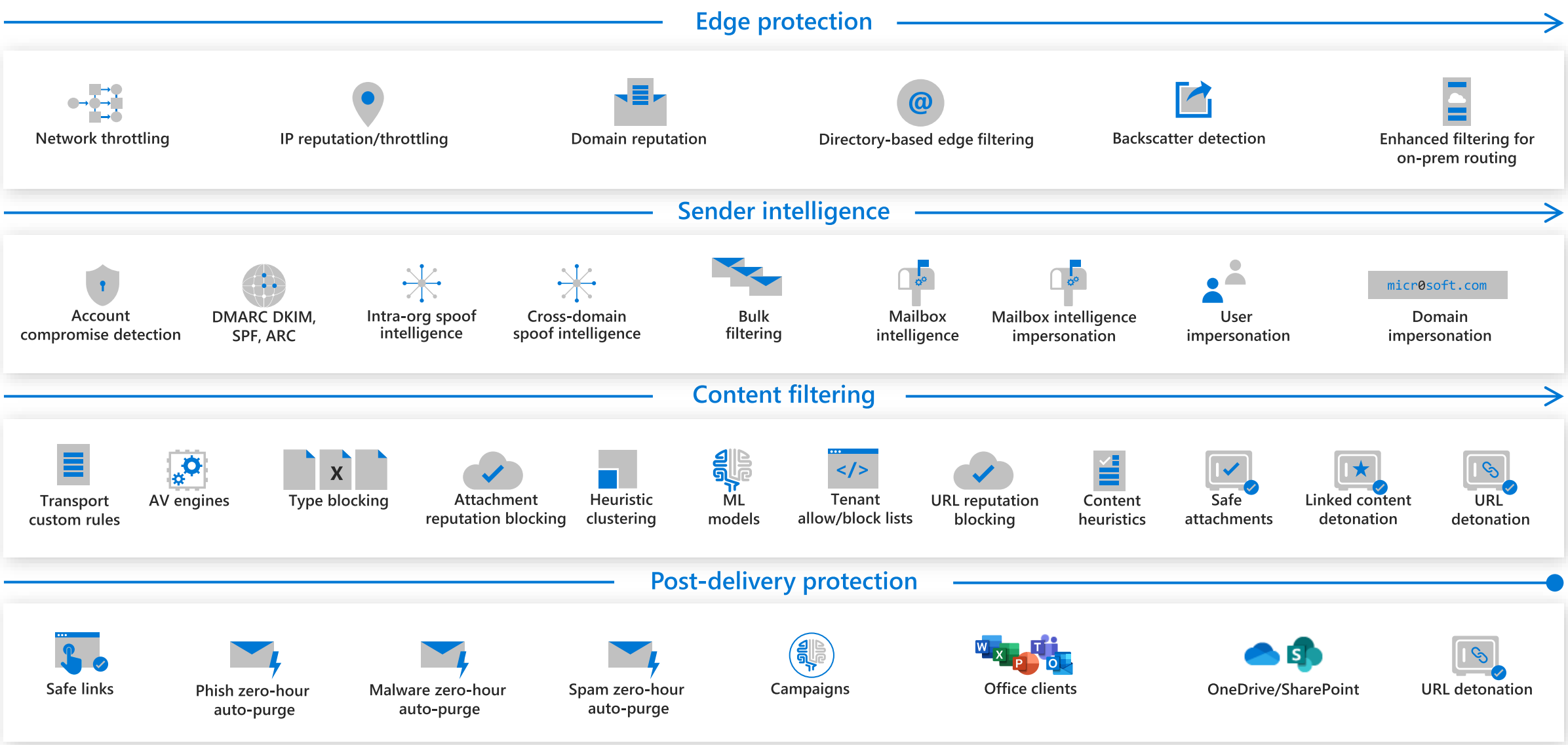


Outbound Filtering



Demo

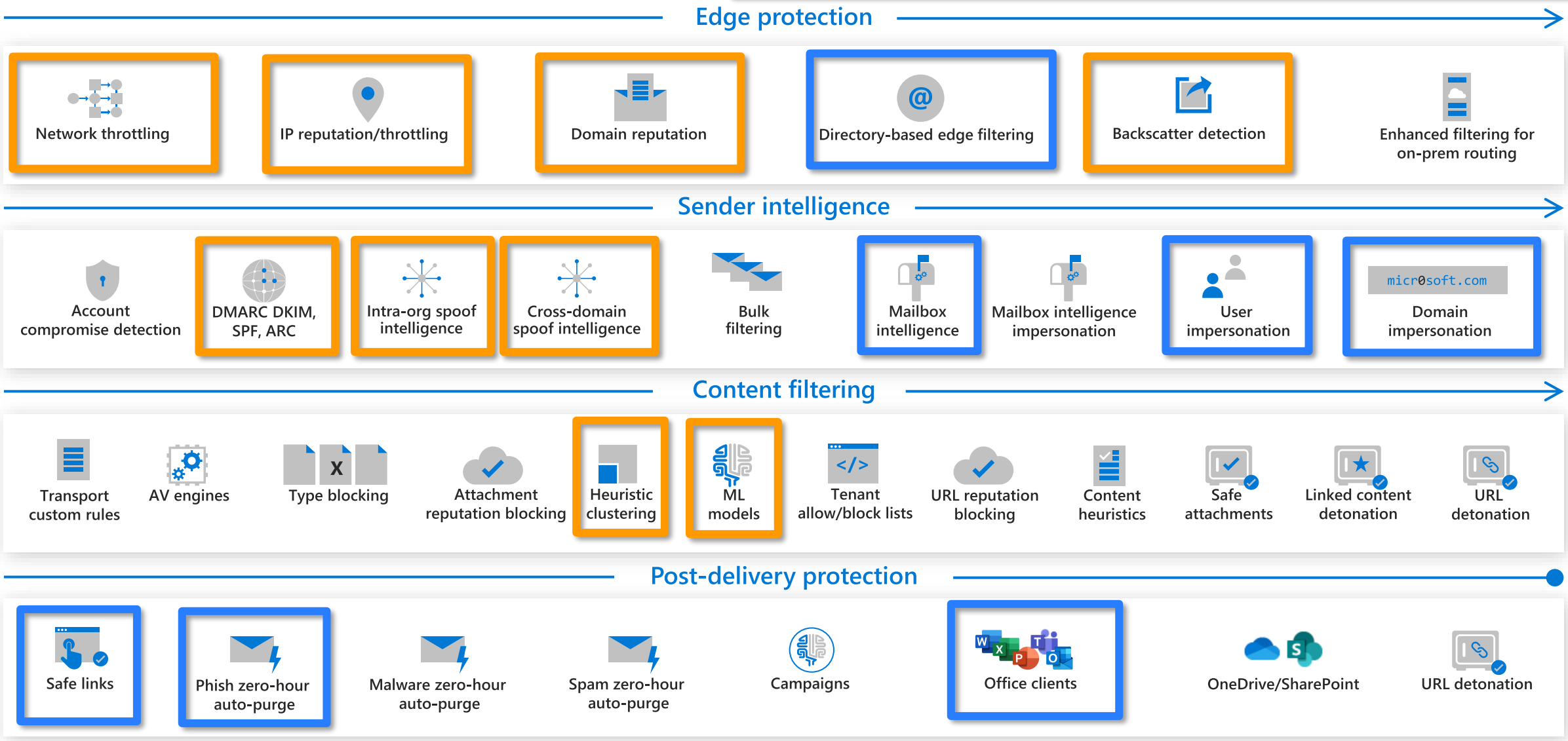
Multi-Layered protection stack

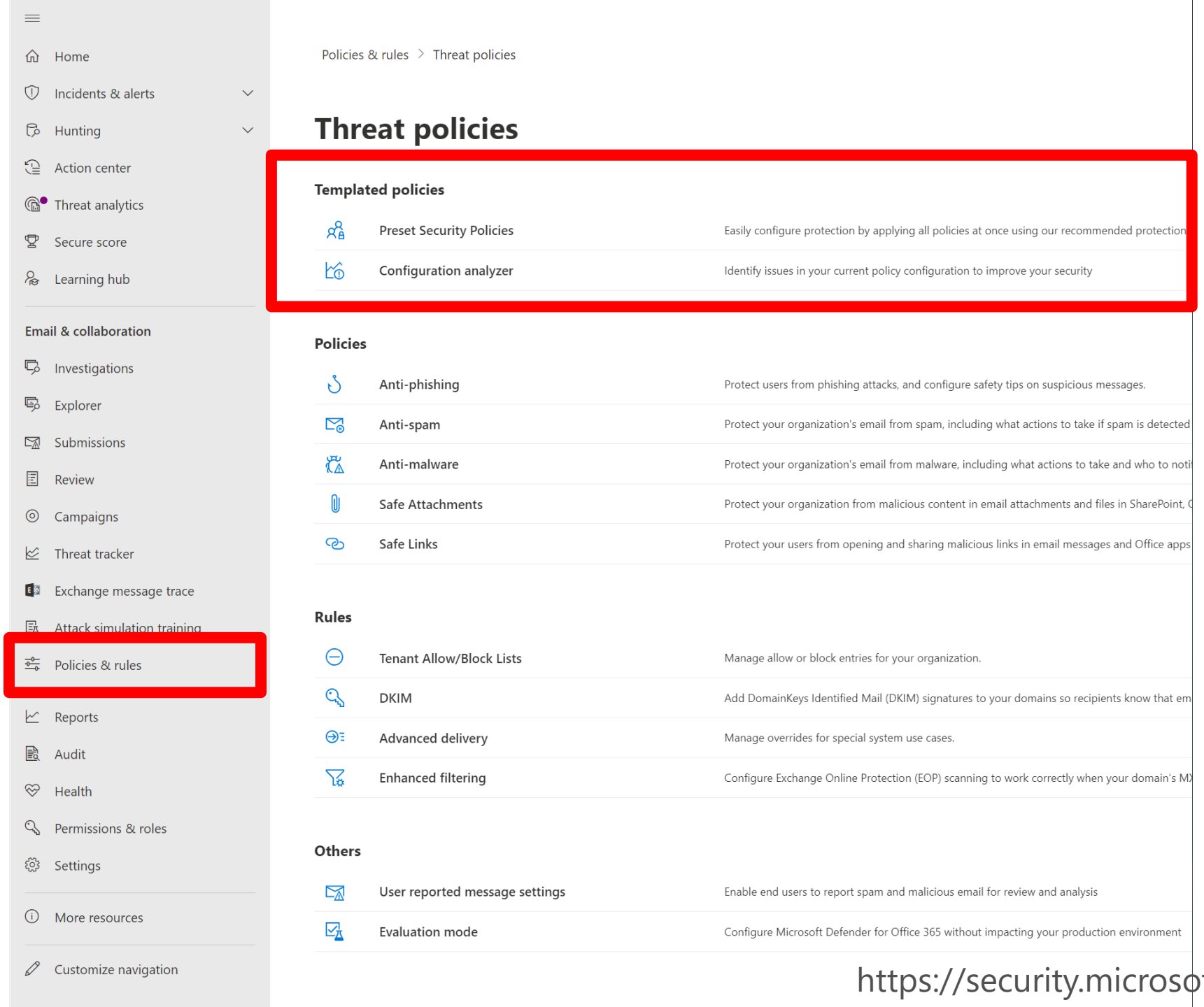


Multi-Layered protection stack

- Requires real sender as part of real mail flow

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





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

- 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

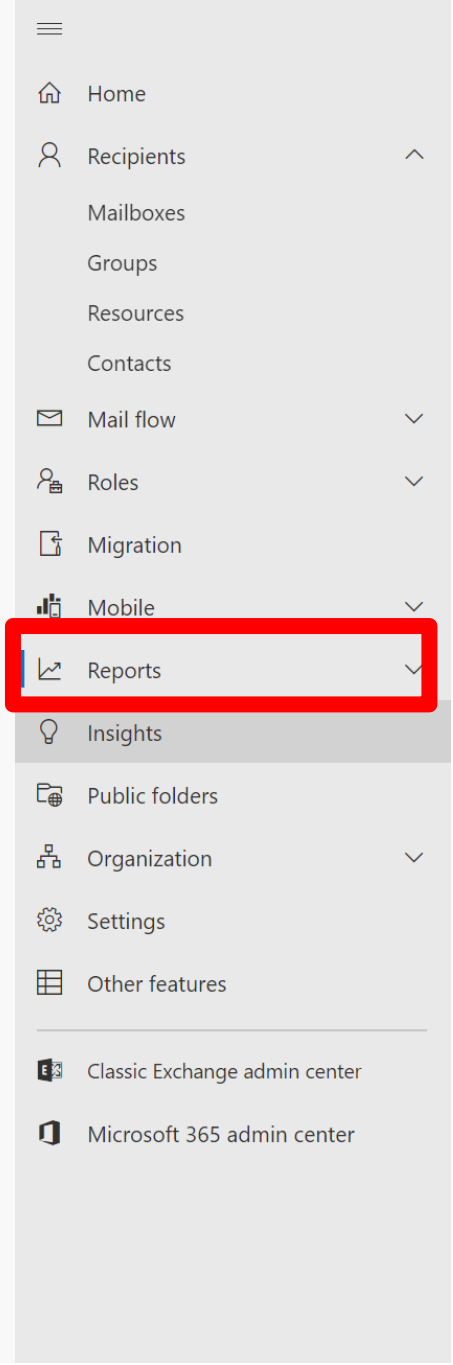
( ) **Link in Attachment**
In this type of technique, which is a hybrid of a Credential Harvest and Malware Attachment, a malicious actor creates a message, with a URL in an attachment, and then inserts the attachment into the message. When the target opens the attachment, they are represented with a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



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 isssues.
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 ure protocol used by devices, such as printers,

https://admin.exchange.microsoft.com/#/reports/mailflowreportsmain

Attack simulation training

Overview | Simulations | Payloads | Simulation auto

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

Draft **0** | Ready **120**

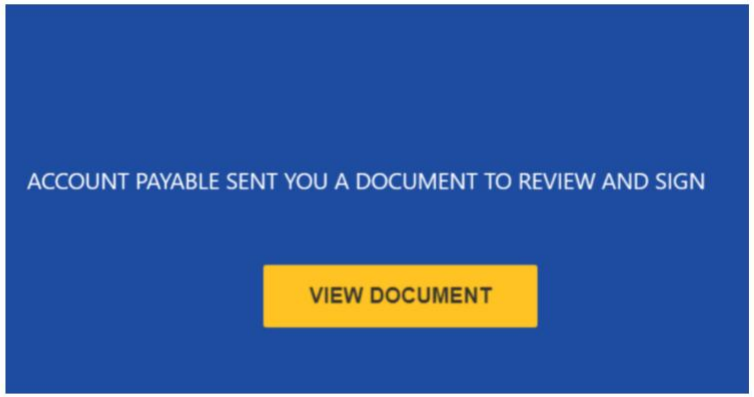
Send a test | Create a payload | Copy payload

Payload name	Type	Source
2 Failed Messages	Social Engineering	Global
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



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

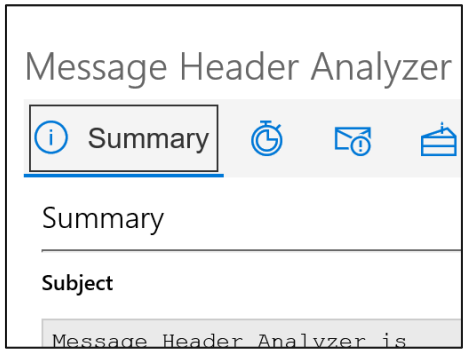
Email subject
Account Payable Sent You A Document To Review And Sign]

Source
Global

Demo

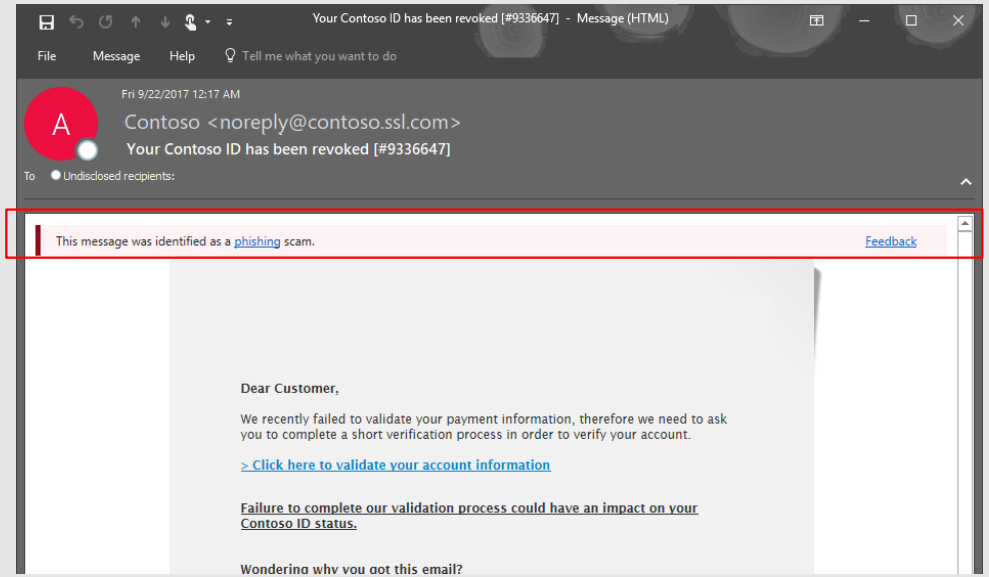
Outlook Add Ins

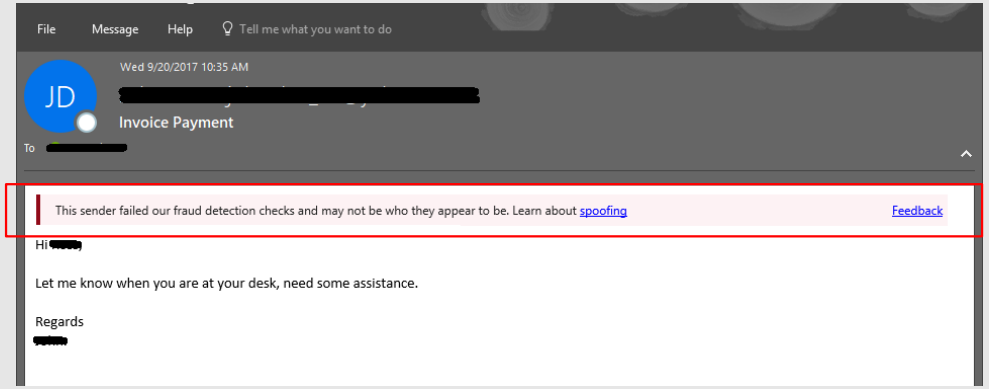
Report Message

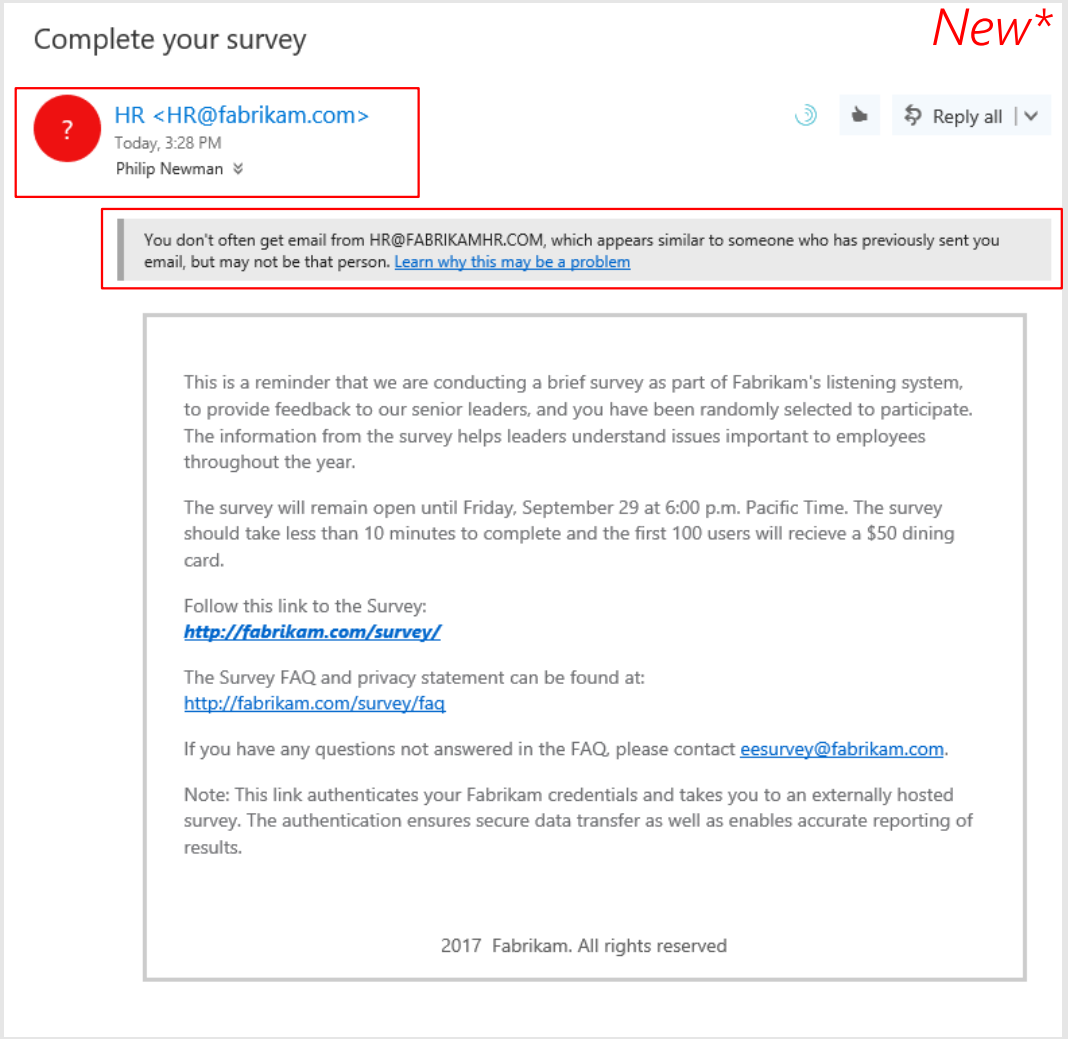


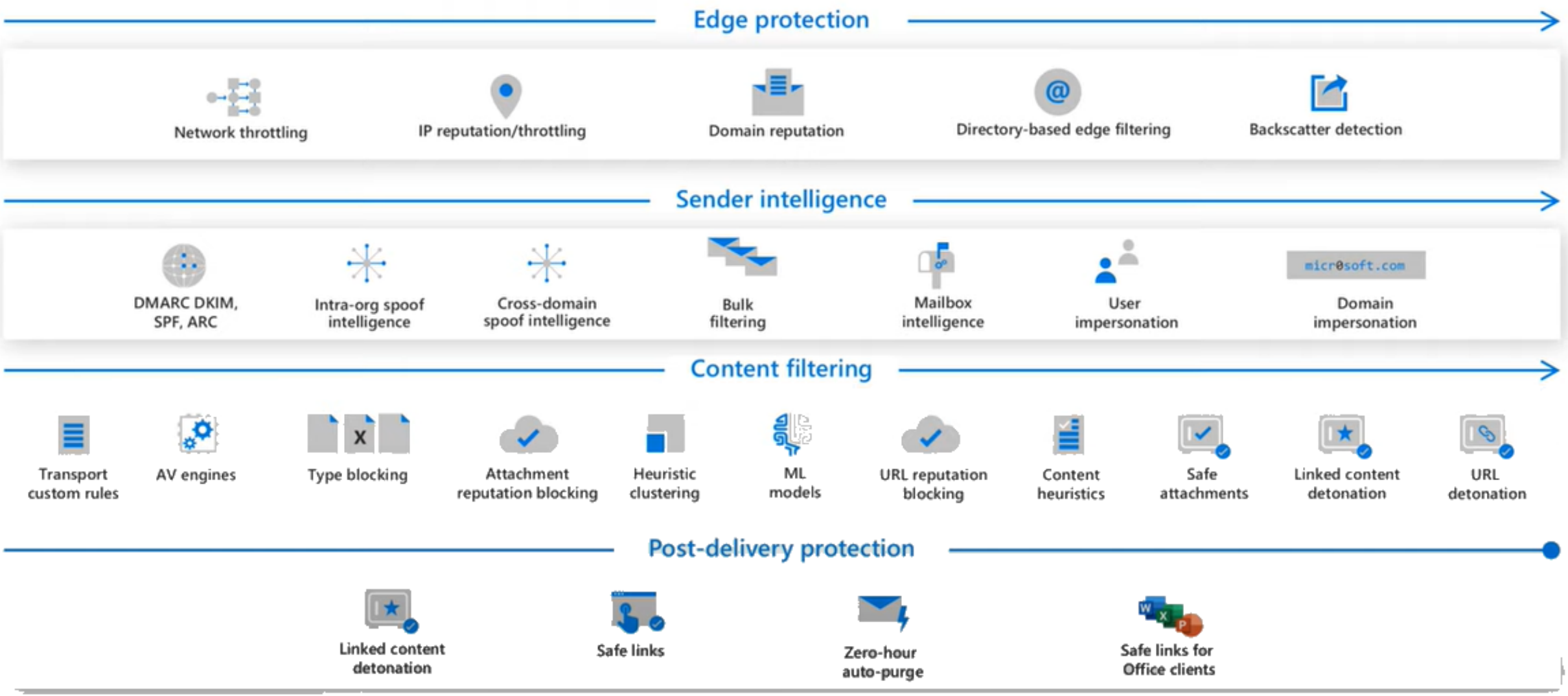
Message Header Analyzer

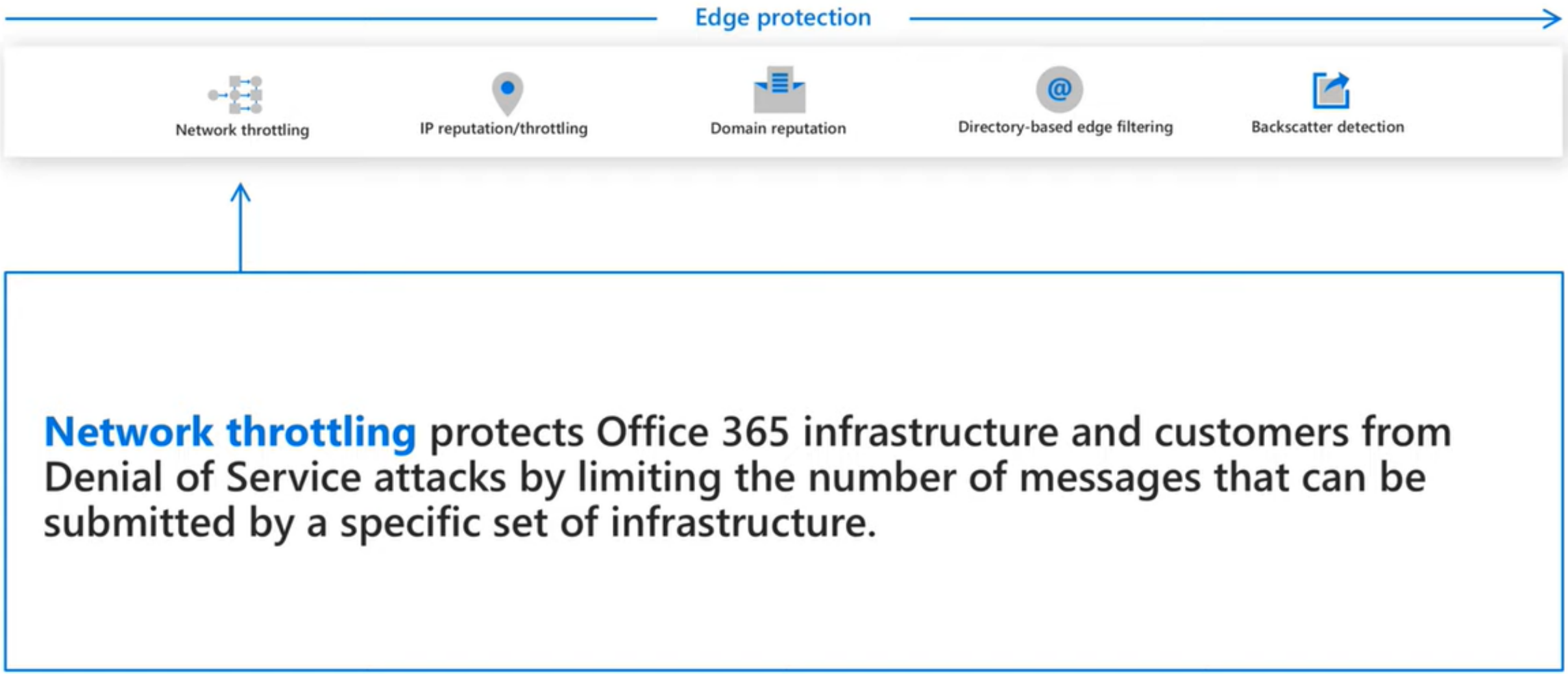
Intelligent Client Tips & Warnings for Suspicious Mails

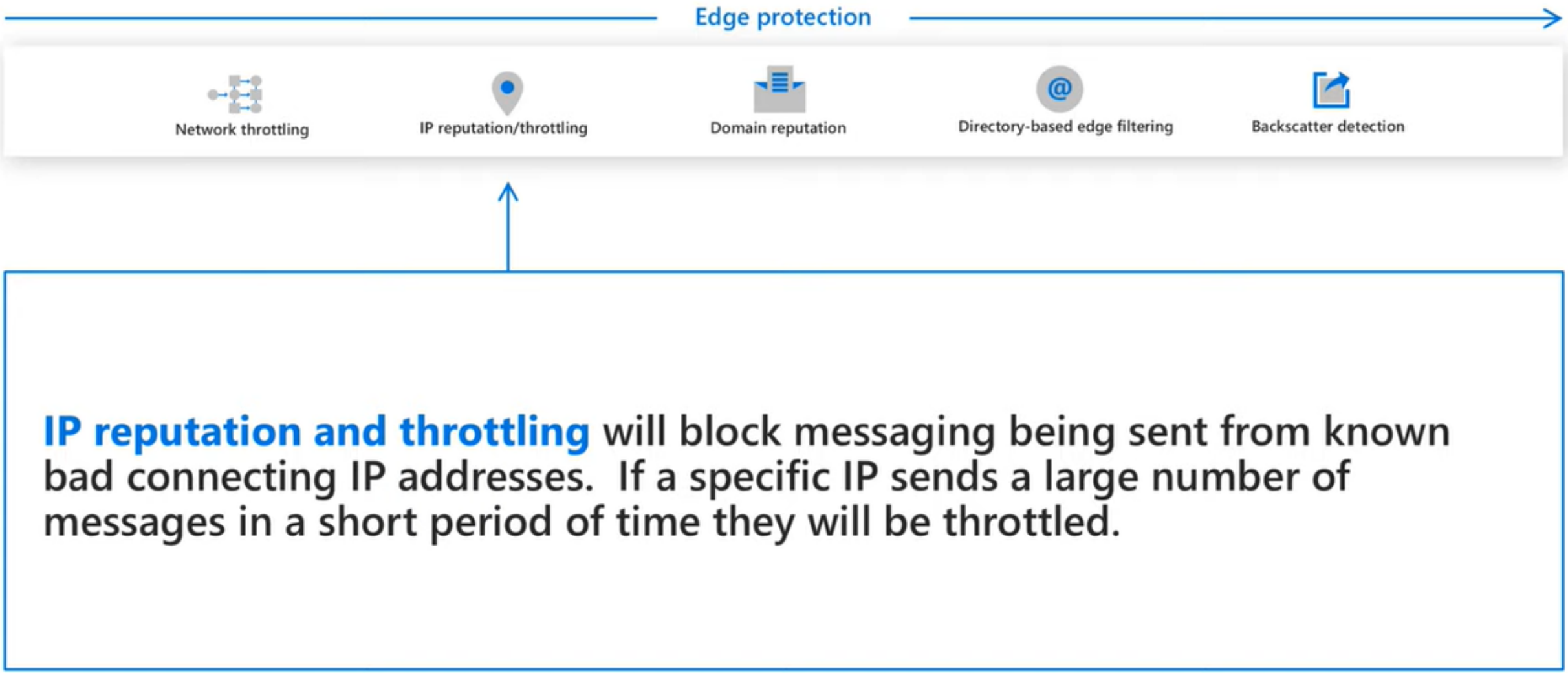


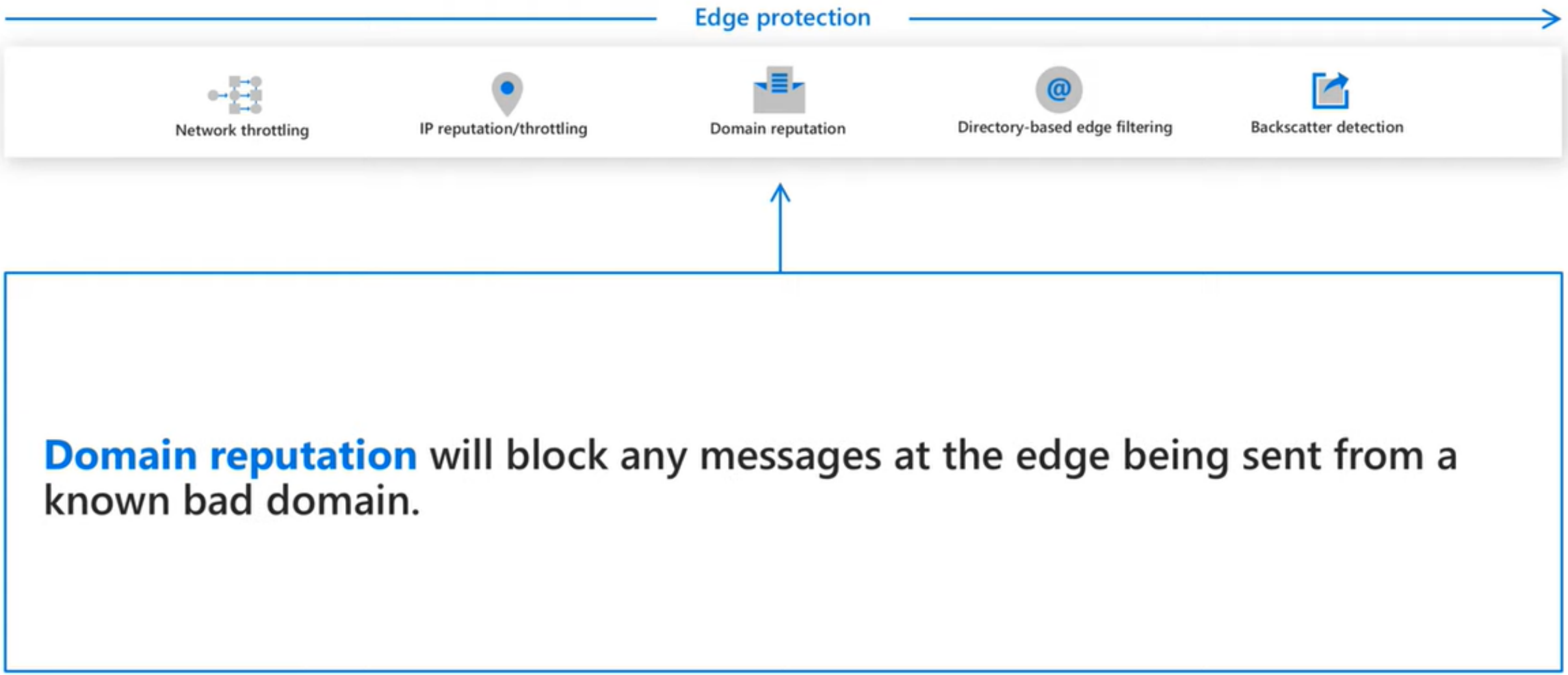


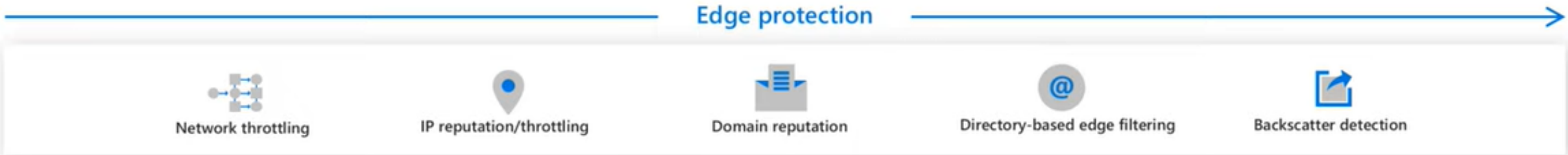



Edge protection
Network throttling
IP reputation/throttling
Domain reputation
Directory-based edge filtering
Backscatter detection
Sender intelligence
DMARC DKIM, SPF, ARC
Intra-org spoof intelligence
Cross-domain spoof intelligence
Bulk filtering
Mailbox intelligence
User impersonation
micr0soft.com
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

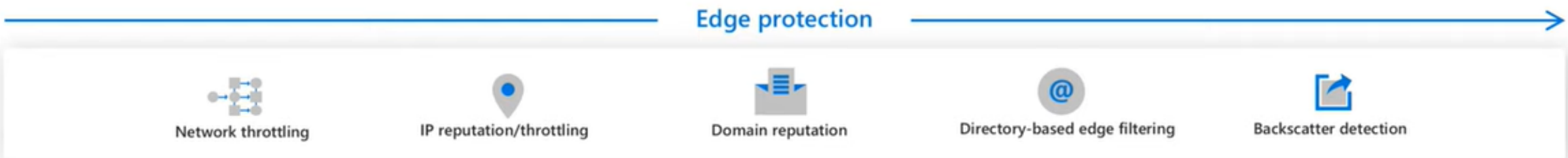

Edge protection
Network throttling
IP reputation/throttling
Domain reputation
Directory-based edge filtering
Backscatter detection
Network throttling protects Office 365 infrastructure and customers from Denial of Service attacks by limiting the number of messages that can be submitted by a specific 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.

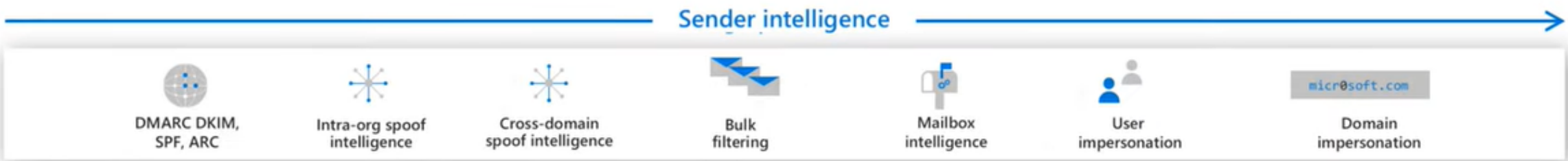

Edge protection
Network throttling
IP reputation/throttling
Domain reputation
Directory-based edge filtering
Backscatter detection
Domain reputation will block any messages at the edge being sent from a known bad domain.



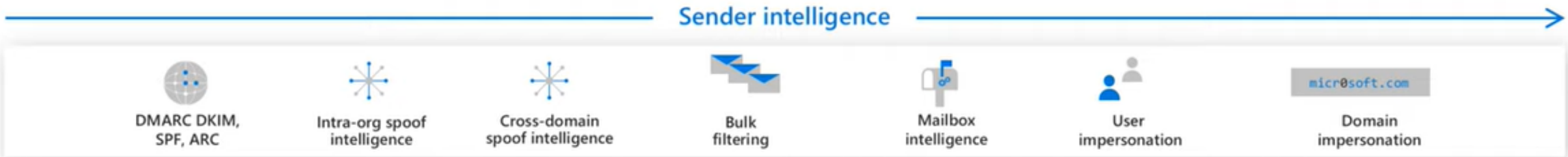
Directory-based edge filtering blocks attempts to harvest an organizations directory information through SMTP.



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



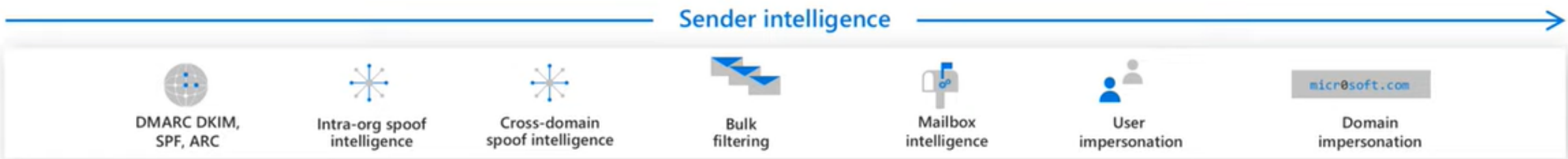
Features within sender intelligence are critical for catching a great deal of spam, bulk, and unauthorized spoof and is an important factor in phish detection. Most of these features are individually configurable.



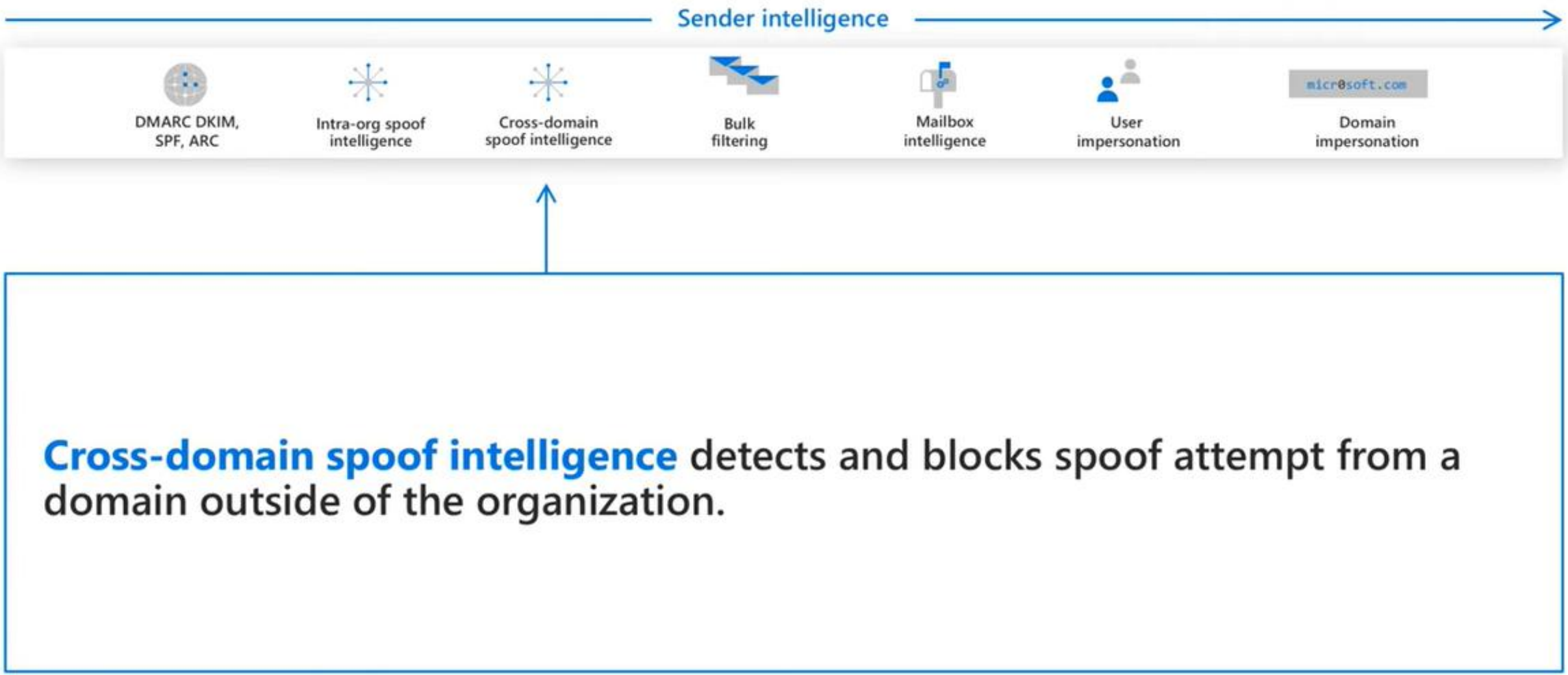
SPF enforces rejecting mails based on which IPs are allowed to send mail on the organizations behalf as define in their DNS record.

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.

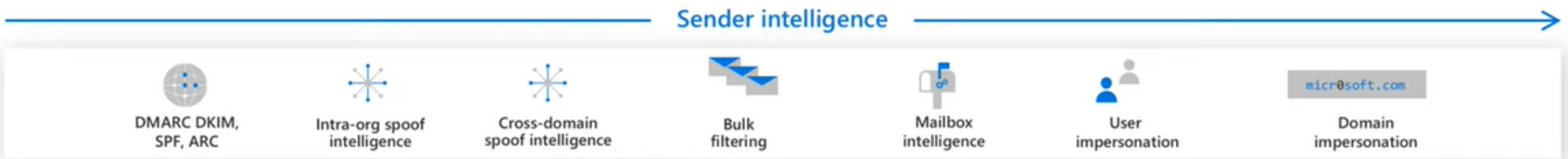


Intra-org spoof intelligence detects and blocks spoof attempt from a domain within the organization.

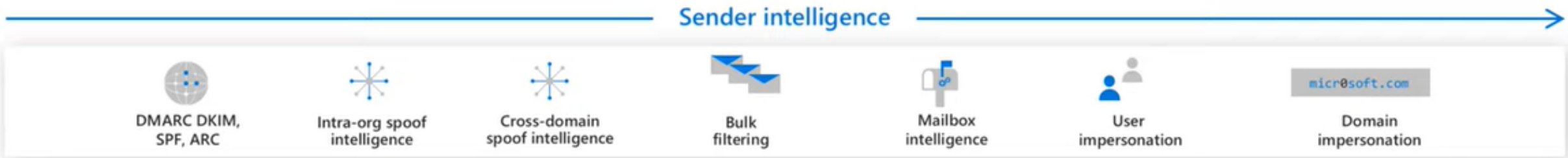

Sender intelligence
DMARC DKIM, SPF, ARC
Intra-org spoof intelligence
Cross-domain spoof intelligence
Bulk filtering
Mailbox intelligence
User impersonation
micr0soft.com
Domain impersonation
Cross-domain spoof intelligence detects and blocks spoof attempt from a domain outside of the organization.

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.

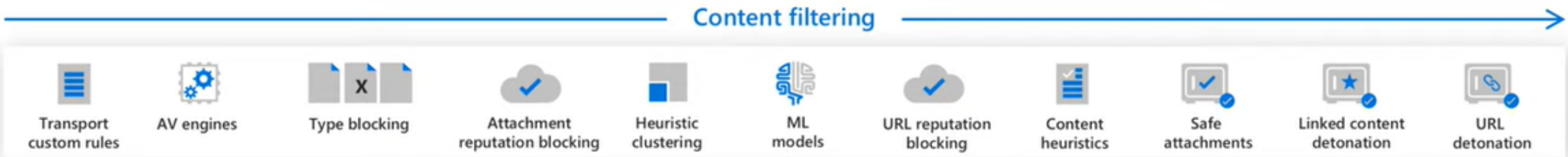
Mailbox intelligence uses each user's communication graph to detect when the sender appears to be someone who usually communicates with them, but in *reality* isn't.



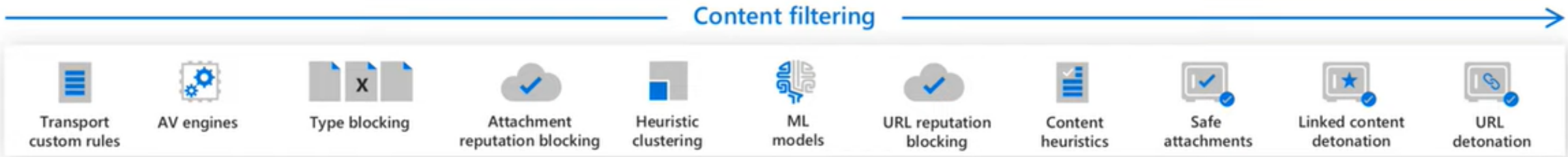
User impersonation allows an admin to provide a list of high value targets that are likely to be impersonated within their organization. If a mail arrives with a sender with the same name, but a different address the recipient is warned.



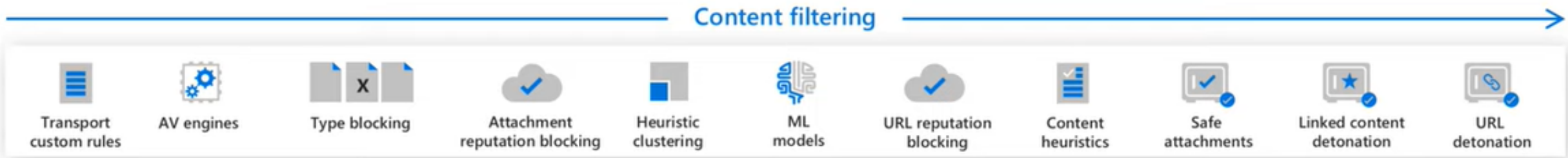
Domain impersonation detect domains that are similar to the recipient's domain, attempting to look like an internal domain.



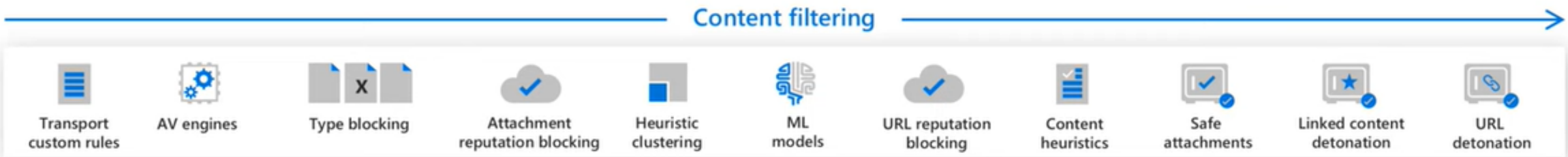
Transport rules also known as ETRs, allow an admin to perform a wide range of complex action when an equally wide range of conditions are met for a given message.



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

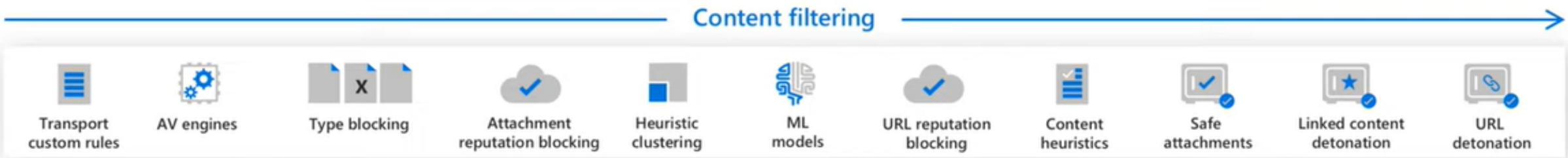


The AV engines are also used to true-type all attachments so that **type blocking** can block all attachment of the types the admin specifies.



Whenever ATP detects a malicious attachment the file's hash and a hash of it's 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.

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.



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

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

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

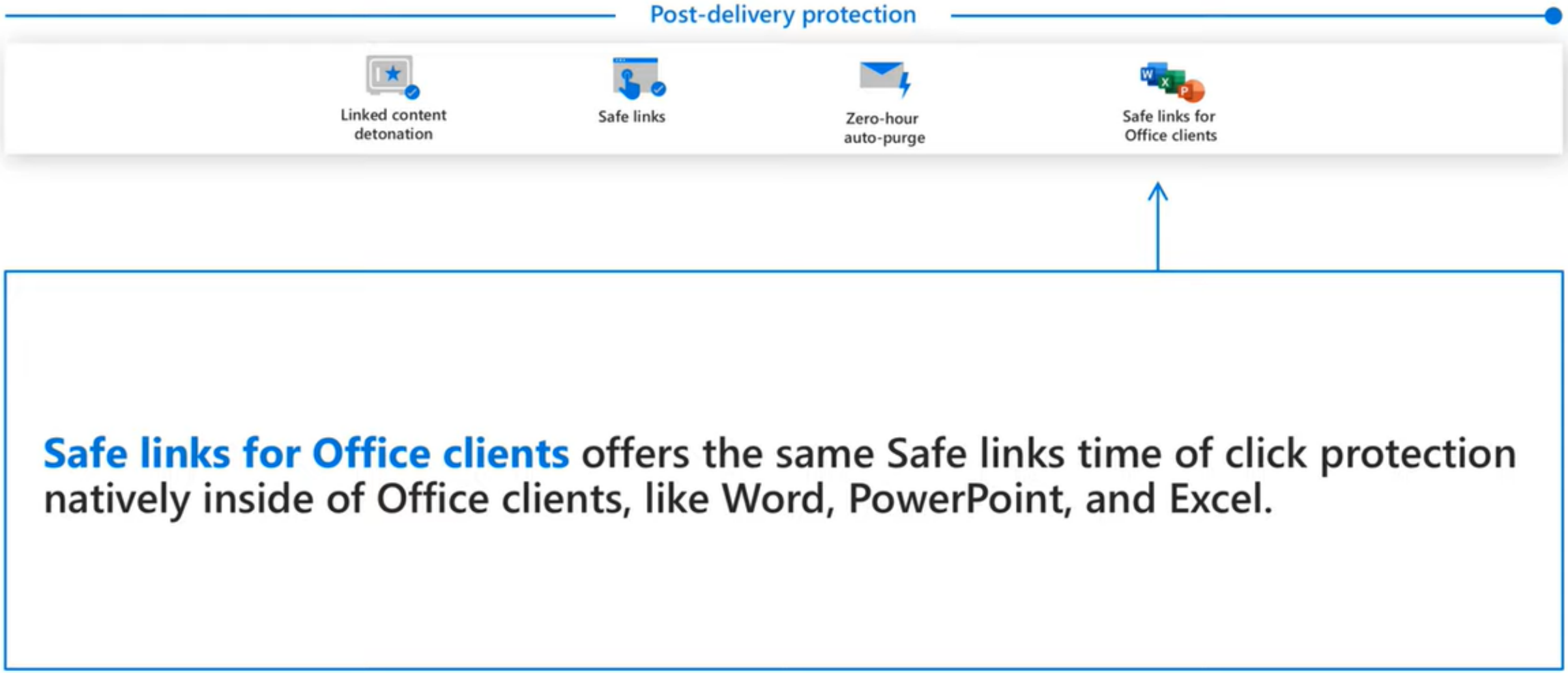
Linked content detonation treats every URL linking to a file in an email as an attachment, asynchronously sandboxing the file at time of delivery.

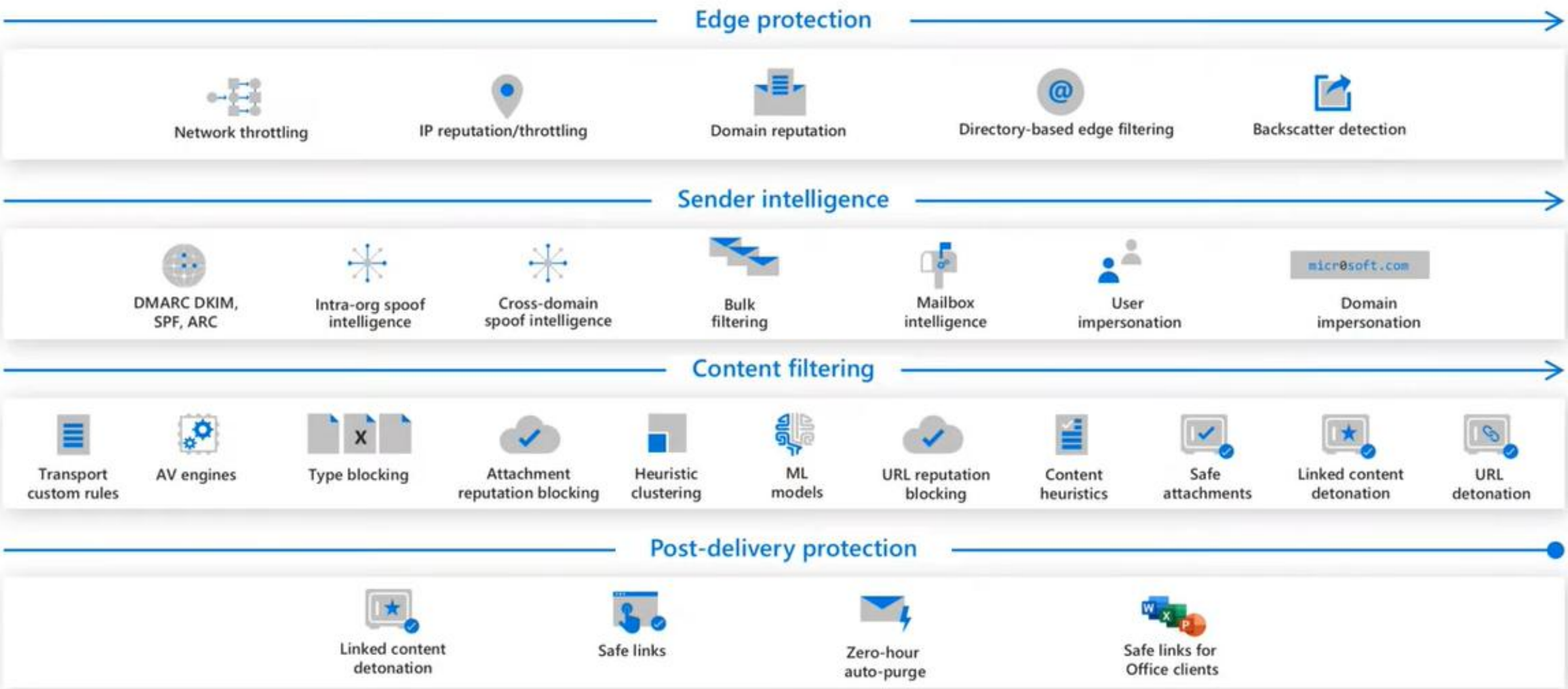
When the upstream anti-phish tech finds a message or URL to be suspicious, **URL detonation** sandboxes the URLs in the message at time of delivery.

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.

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.

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
micr0soft.com
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

Message Header Analyzer
https://appsource.microsoft.com/en-us/product/office/WA104005406

Report message

https://appsource.microsoft.com/en-us/product/office/WA104381180?tab=Overview