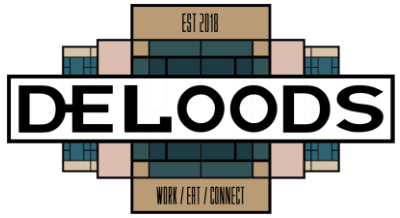
PROTECTING YOUR EMAIL ENVIRONMENT USING EXCHANGE ONLINE PROTECTION & MICROSOFT DEFENDER FOR OFFICE

Kenneth van Surksum



Many thanks to our

Sponsors

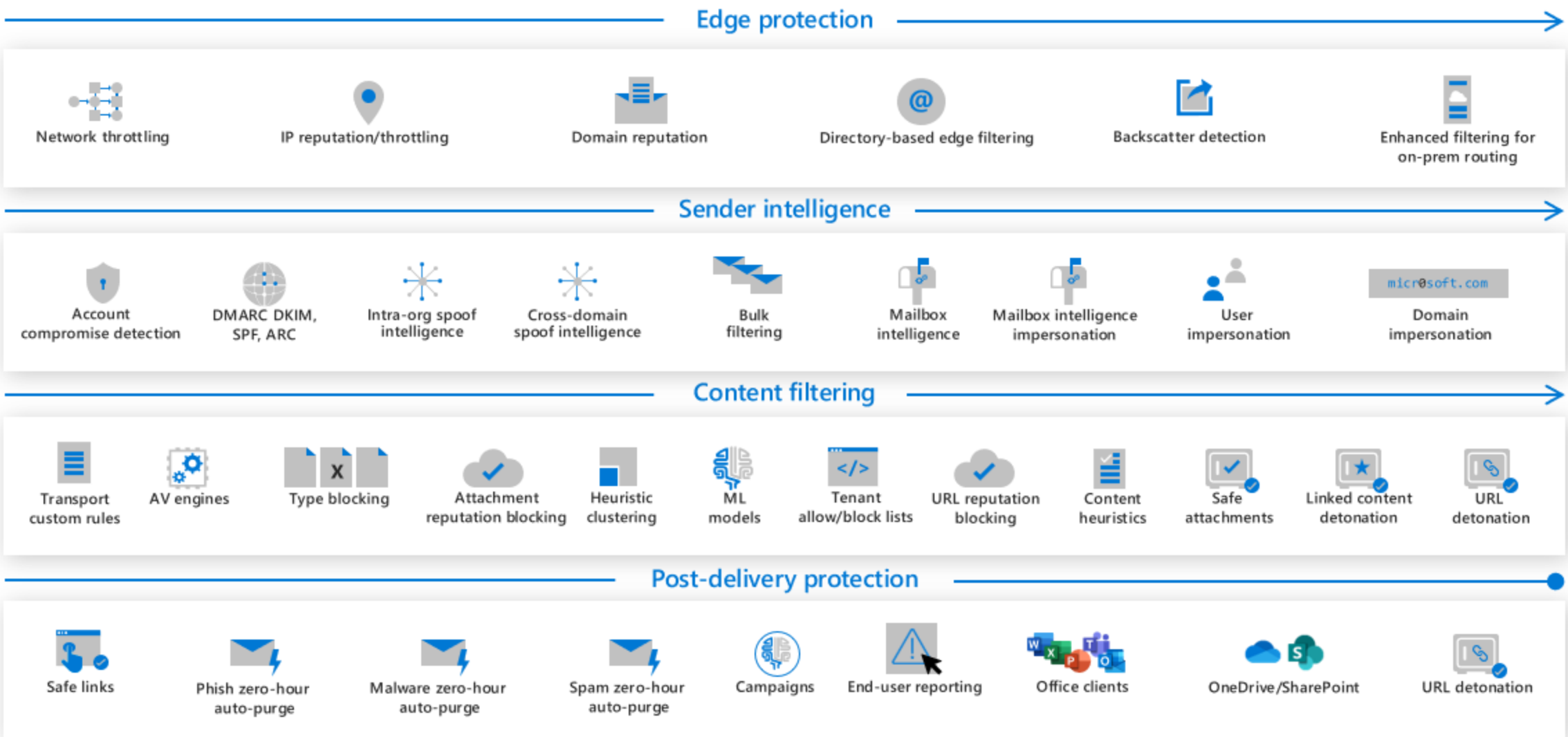
EXCHANGE ONLINE PROTECTION AND MICROSOFT DEFENDER FOR OFFICE

A CARWASH FOR YOUR INCOMING EMAIL

SERVICE LEVEL AGREEMENT

Service Level Agreements (SLAs) and support	
Spam effectiveness SLA	> 99%
False positive ratio SLA	< 1:250.000
Virus detection and blocking SLA	100% of known viruses
Monthly uptime SLA	99,999%

Microsoft Defender for Office 365 protection stack




SNIPER
VS
SHOTGUN

About “Kenneth van Surksum”

Focus

Modern Workplace Consultant, Microsoft Certified Trainer, Co-founder and organizer at Workplace Ninja User Group Netherlands

From

The Netherlands

My Blog

https://www.vansurksum.com

Certifications

Microsoft 365 Certified Enterprise Administrator

Microsoft Certified Azure Solutions Architect

Hobbies

Cooking on my Kamado Joe & Sports

Contact

kenneth@vansurksum.com

https://twitter.com/kennethvs

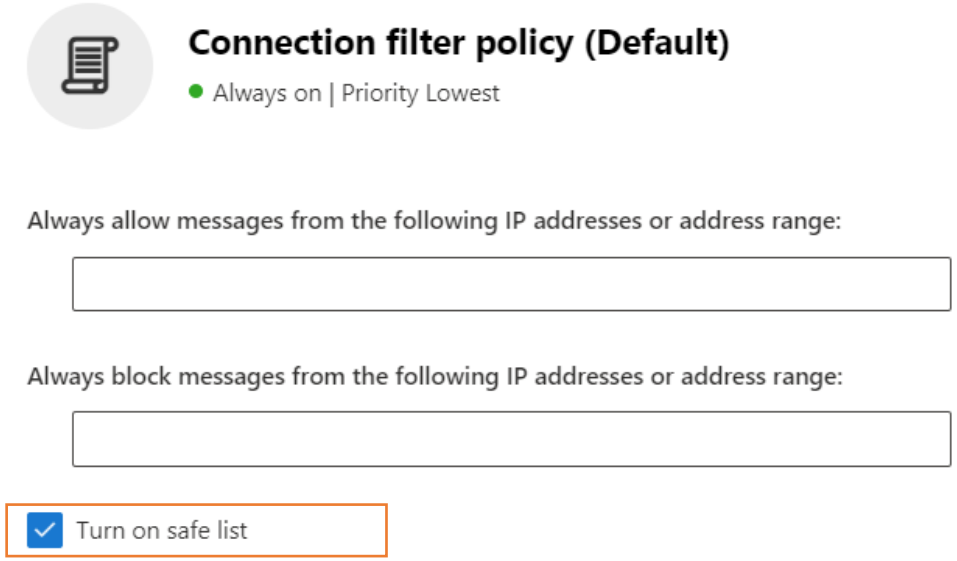
https://www.linkedin.com/in/kennethvansurksum

Email Flow


KNOW THE ANGLES, WASH STAGES AND RECOMMENDED ANGLE RANGE
Presoak
50° to 110°
Undercarriage
50° to 110°
Wash
50° to 110°
Rinse
40° to 80°
Wax
25° to 65°
Final Rinse
40° to 110°
Touchless
In-Bay Automatic
5° to 15°
Self-Serve
25° to 40°

PHASE 1: CONNECTION FILTERING

- Checks for sender reputation
- Blocks most of the bad mail
- Can be found under Anti-spam policies



https://sender.office.com

Office 365

Office 365 Anti-Spam IP Delist Portal

Display language: English (Unite

If you're trying to send mail to an Office 365 recipient and the mail has been rejected because of your sending IP add
steps to submit a delisting request.

Senders are responsible for making sure that their mail from this IP address isn't abusive or malicious.

Learn More

Step 1: Send verification — Step 2: Confirm email address — 3. Delist IP

Step 1: Provide your email address and the IP address you want to delist so they can be verified.

Email address

IP address

Enter the characters you see

New | Audio

Submit

IP Delisting

- Visit https://sender.office.com

- Fingers crossed

PHASE 2: ANTI MALWARE

- Prevents:
  - Broad attacks
  - Volume based attacks
  - Known attacks
- Cannot be disabled

- Zero-day Malware protection -> MDO

PHASE 3: POLICY FILTERING

- Mail flow rules a.k.a. transport rules

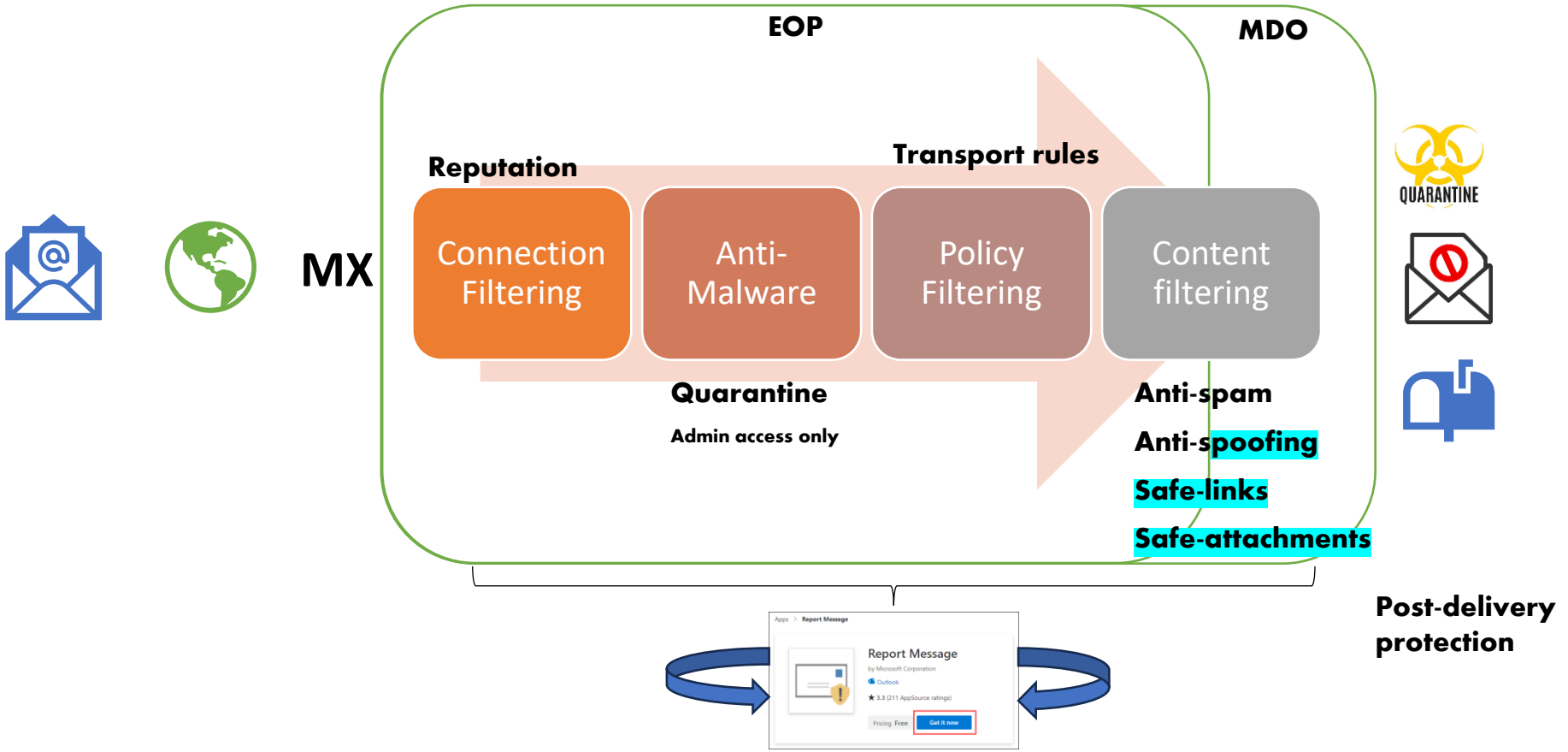
- Use them to whitelist and not the default methods like Safe Senders/Safe Domains in Anti-Spam policies, tenant allow or connection filters.

PHASE 4: CONTENT FILTERING

Messages are identified as spam, high confidence spam, phishing, high confidence phishing, or bulk (anti-spam policies) or spoofing (spoof settings in anti-phishing policies).

- Anti-spam
- Anti-spoofing
- Safe Links*
- Safe Attachments*

Email flow with EOP and MDO



Skip policy processing

Policies & rules > Threat policies > Advanced delivery

Advanced delivery

Specify dedicated mailboxes that are used by security teams to collect and analyze unfiltered messages (both good and bad). Email sent to these mailboxes is delivered unfiltered. Learn more

SecOps mailbox | Phishing simulation

Edit | Refresh

Display name	Email
Security Operations	secops@vansurksum.com

Microsoft Defender for Office

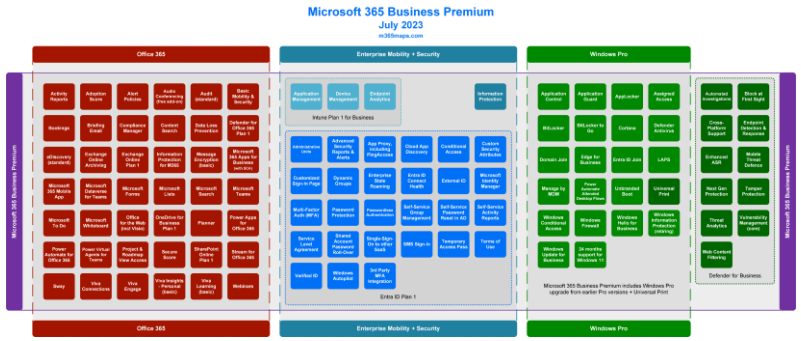
- (Soon to be) renamed to Microsoft 365 Defender XDR for Office 365
- Protects from Zero-day malware, phish and business email compromise (BEC)
- Safe attachments
  - Also for SPO, OneDrive, Teams)
- Safe Links
- Advanced phishing protection
- Real-time detections

Licensing

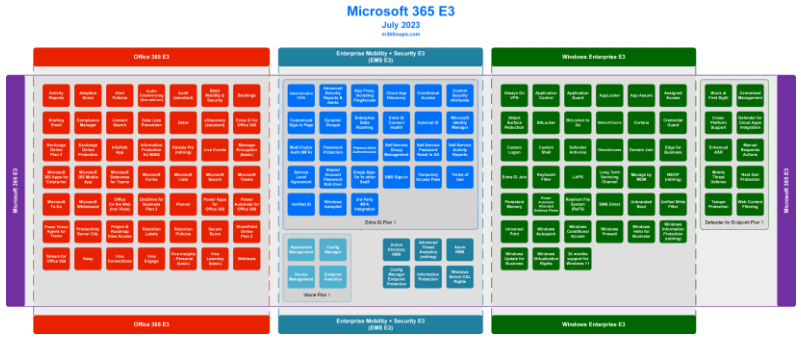
Protection level	Description
EOP	Prevents broad, volume-based, known attacks.
Defender for Office 365 P1	Protects email and collaboration from zero-day malware, phish, and business email compromise.
Defender for Office 365 P2	Adds post-breach investigation, hunting, and response, as well as automation, and simulation (for training).

Part of suite licensing

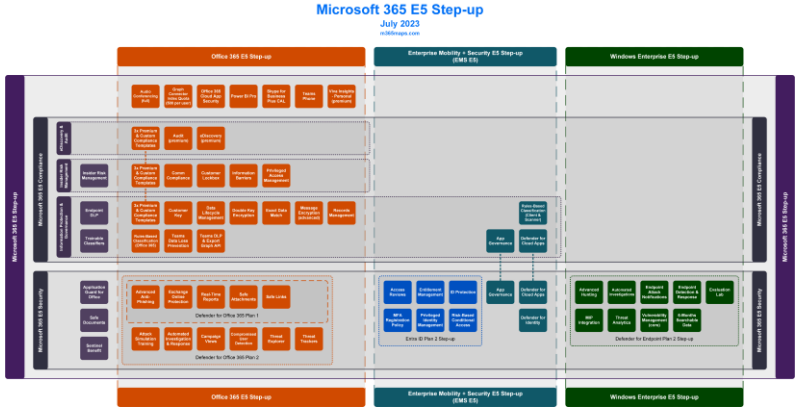
M365 Business Premium includes MDO P1



M365 E3 **doesn't** include MDO



M365 E5 includes MDO P2



Source: https://m365maps.com

Safe Attachments

Global settings

Use this page to protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Microsoft Teams.

Protect files in SharePoint, OneDrive, and Microsoft Teams

If a file in any SharePoint, OneDrive, or Microsoft Teams library is identified as malicious, Safe Attachments will prevent users from opening and downloading the file. Learn more

Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams

Help people stay safe when trusting a file to open outside Protected View in Office applications.

Before a user is allowed to trust a file opened in a supported version of Office, the file will be verified by Microsoft Defender for Endpoint. Learn more about Safe Documents.

Turn on Safe Documents for Office clients. Only available with *Microsoft 365 E5* or *Microsoft 365 E5 Security* license. Learn more about how Microsoft handles your data.

Allow people to click through Protected View even if Safe Documents identified the file as malicious

Save Cancel

Safe Attachments unknown malware response

Select the action for unknown malware in attachments. Learn more

Warning

- **Monitor** and **Block** actions might cause a significant delay in message delivery. Learn more
- **Dynamic Delivery** is only available for recipients with hosted mailboxes.
- For **Block** or **Dynamic Delivery**, messages with detected attachments are quarantined and can be released only by an admin.

- ○ Off - Attachments will not be scanned by Safe Attachments.
- ○ Monitor - Deliver the message if malware is detected and track scanning results.
- ◉ Block - Block current and future messages and attachments with detected malware.
- ○ Dynamic Delivery (Preview messages) - Immediately deliver the message without attachments. Reattach files after scanning is complete.

Quarantine policy

AdminOnlyAccessPolicy

Permission to release quarantined messages will be ignored for messages with malware detected and we will fall back to release request instead

Redirect messages with detected attachments

Enable redirect only supports the Monitor action. Learn more

☑ Enable redirect ⓘ

Send messages that contain monitored attachments to the specified email address.

secops@itgration.nl

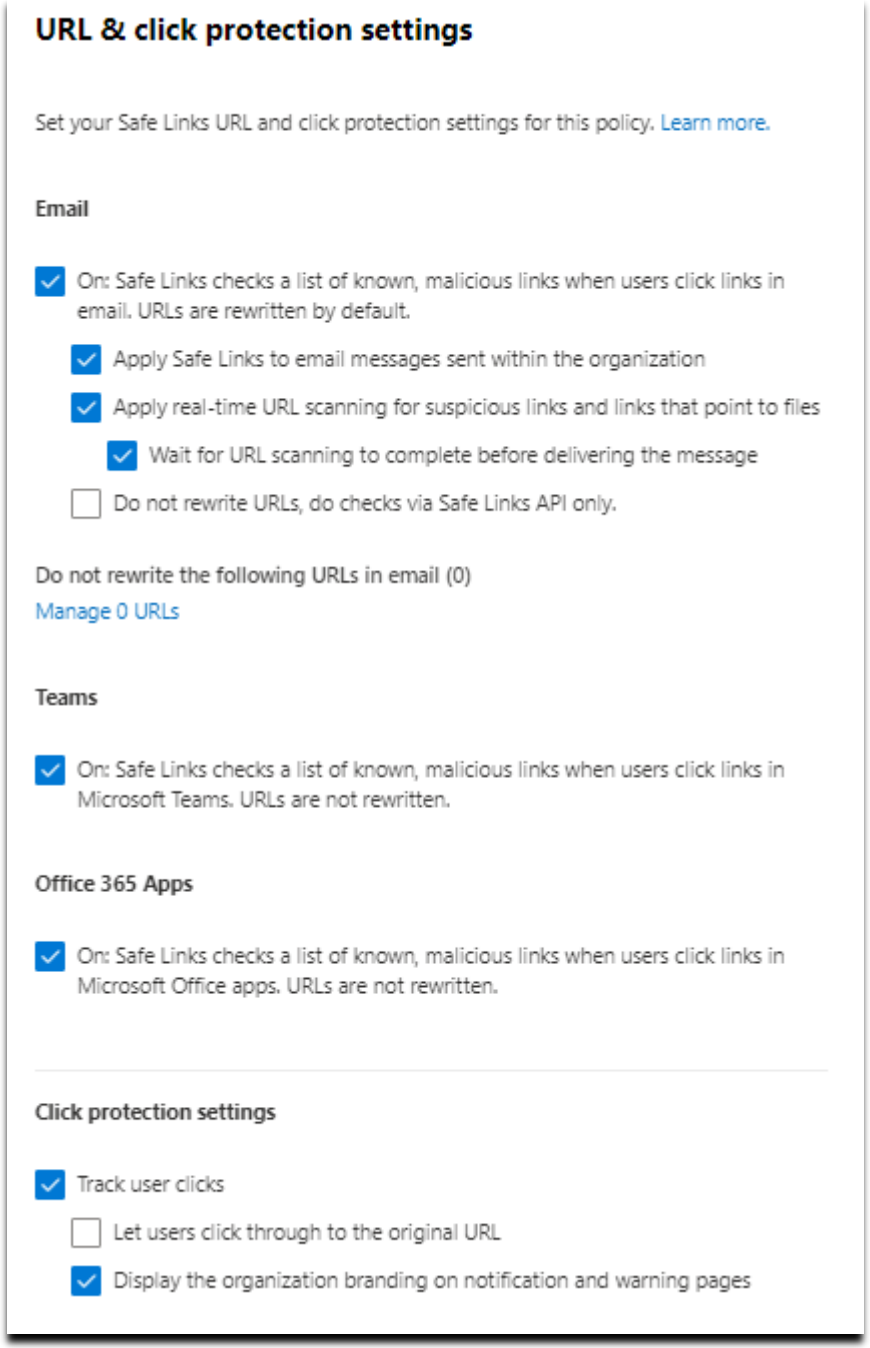
Safe Attachments

- It routes all messages and attachments that do not have a virus/malware signature (= Zero day) to a special environment
- Uses machine learning and analysis techniques to detect malicious intent.
- Basically, Microsoft quickly spins on a Virtual Machine and executes the content carefully watching for suspicious activity.

- You can exclude specific messages from being checked by ATP Safe Links policy, by creating a transport rule which sets the **X-MS-Exchange-Organization-SkipSafeAttachmentProcessing** header to the value **1**.

Safe Links

- If you enable ATP Safe Links, URLs in emails are rewritten to include https://*.safelinks.protection.outlook.com/?url= in front of the original URL.
- Use https://www.o365atp.com/ to decode URLs
- Test using: http://www.spamlink.contoso.com
- Be careful with long URLs (>2048 characters)
- You can exclude specific messages from being checked by ATP Safe Links policy, by creating a transport rule which sets the **X-MS-Exchange-Organization-SkipSafeLinksProcessing** header to the value **1**



DEMO

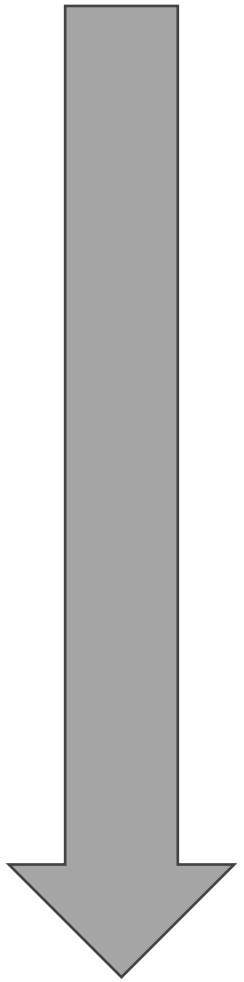
Safe Links

EUROPEAN
MCT SUMMIT 2024
THE NETHERLANDS

Order

1. Malware | CAT:MALW
2. High-confidence Phish | CAT:HPHSH
3. Phishing | CAT:PHSH
4. High-confidence SPAM | CAT:HSPM
5. Spoofing | CAT:SPOOF
6. User Impersonation* | CAT:UIMP
7. Domain Impersonation* | CAT: DIMP
8. Mailbox Intelligence* | CAT:GIMP
9. SPAM | CAT:SPM
10. Bulk |CAT:BULK

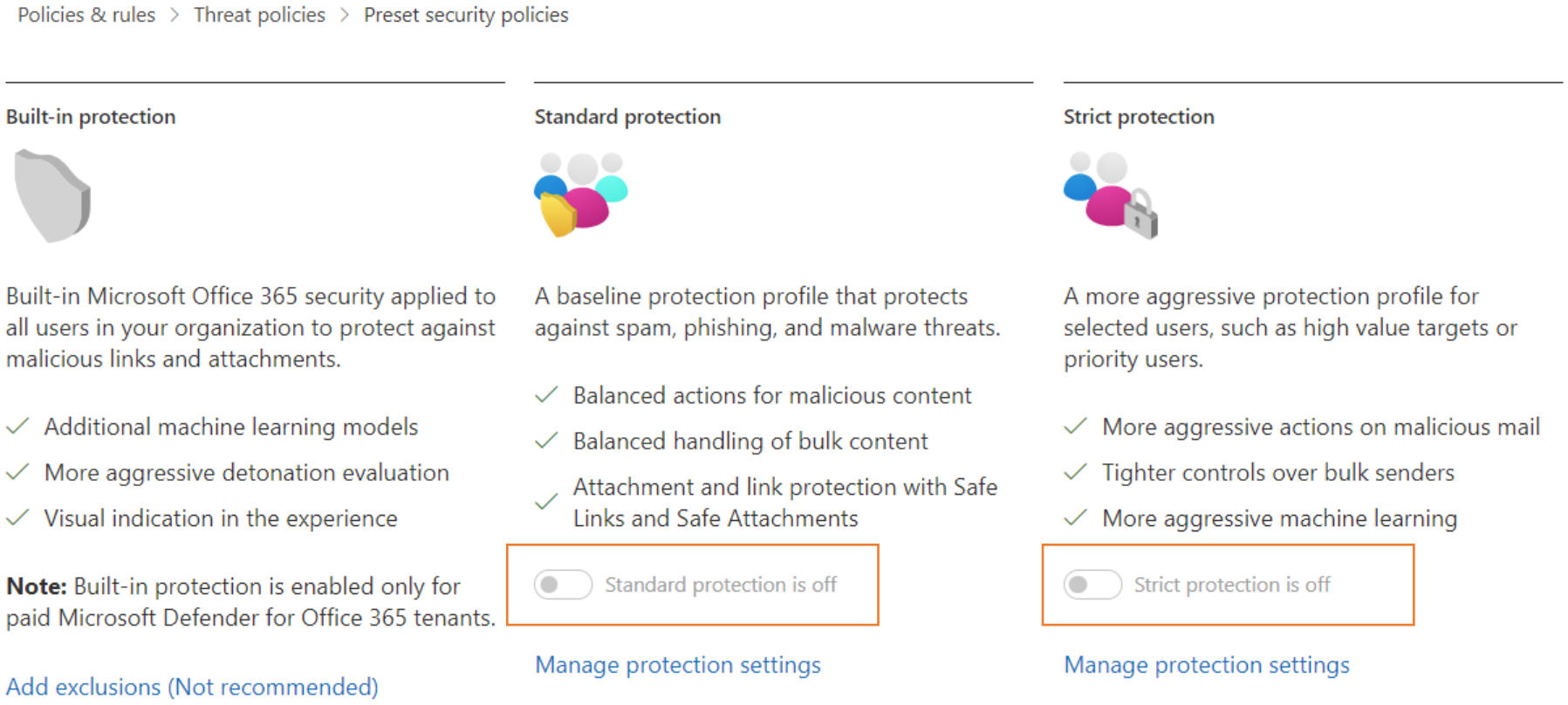
* MDO

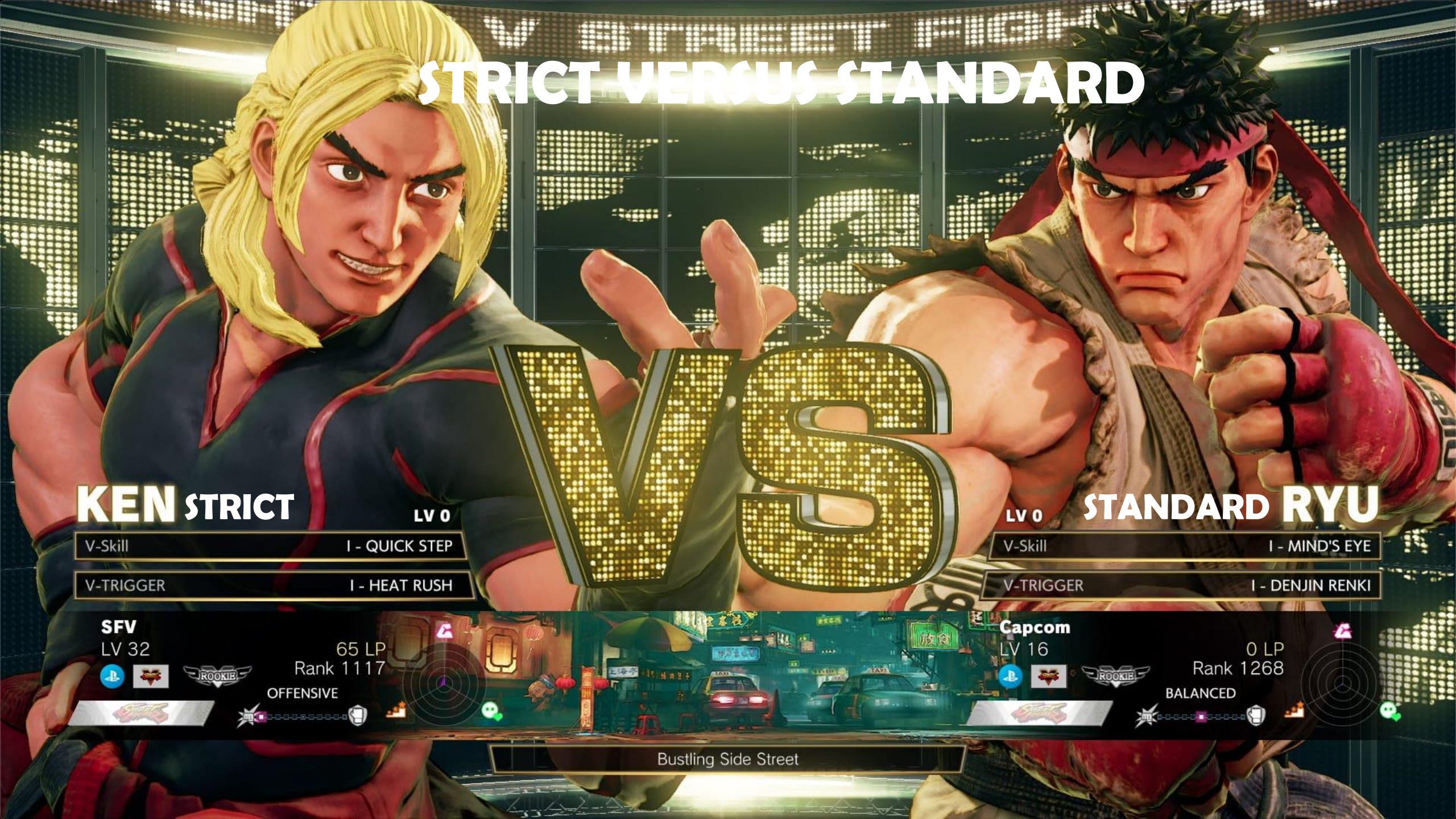


Priority

- **First**: Preset Security Policies
  - Standard
  - Strict
- **Second**: Custom policies
  - Lowest priority wins
- **Always last**: Built-in policies

Only the first hit policy gets applied




STRICT VERSUS STANDARD
KEN STRICT
LV 0
V-Skill
I - QUICK STEP
V-TRIGGER
I - HEAT RUSH
VS
LV 0
STANDARD RYU
V-Skill
I - MIND'S EYE
V-TRIGGER
I - DENJIN RENKI
SFV
LV 32
ROOKIE
65 LP
Rank 1117
OFFENSIVE
Capcom
LV 16
ROOKIE
0 LP
Rank 1268
BALANCED
Bustling Side Street

Recommended settings

[Microsoft recommendations for EOP and Defender for Office 365 security settings]

- https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365?view=o365-worldwide

ORCA

Microsoft Defender for Office 365 Recommended

☆ ☆ ☆ ☆ ☆

Configuration Analyzer Report

Version 2.8.1

This report details any tenant configuration changes recommended within your tenant.

Informational	Recommendations	OK
1	24	41

Configuration analyzer

The Configuration analyzer can help identify issues in your current configuration, and help improve your policies for better security. Learn more.

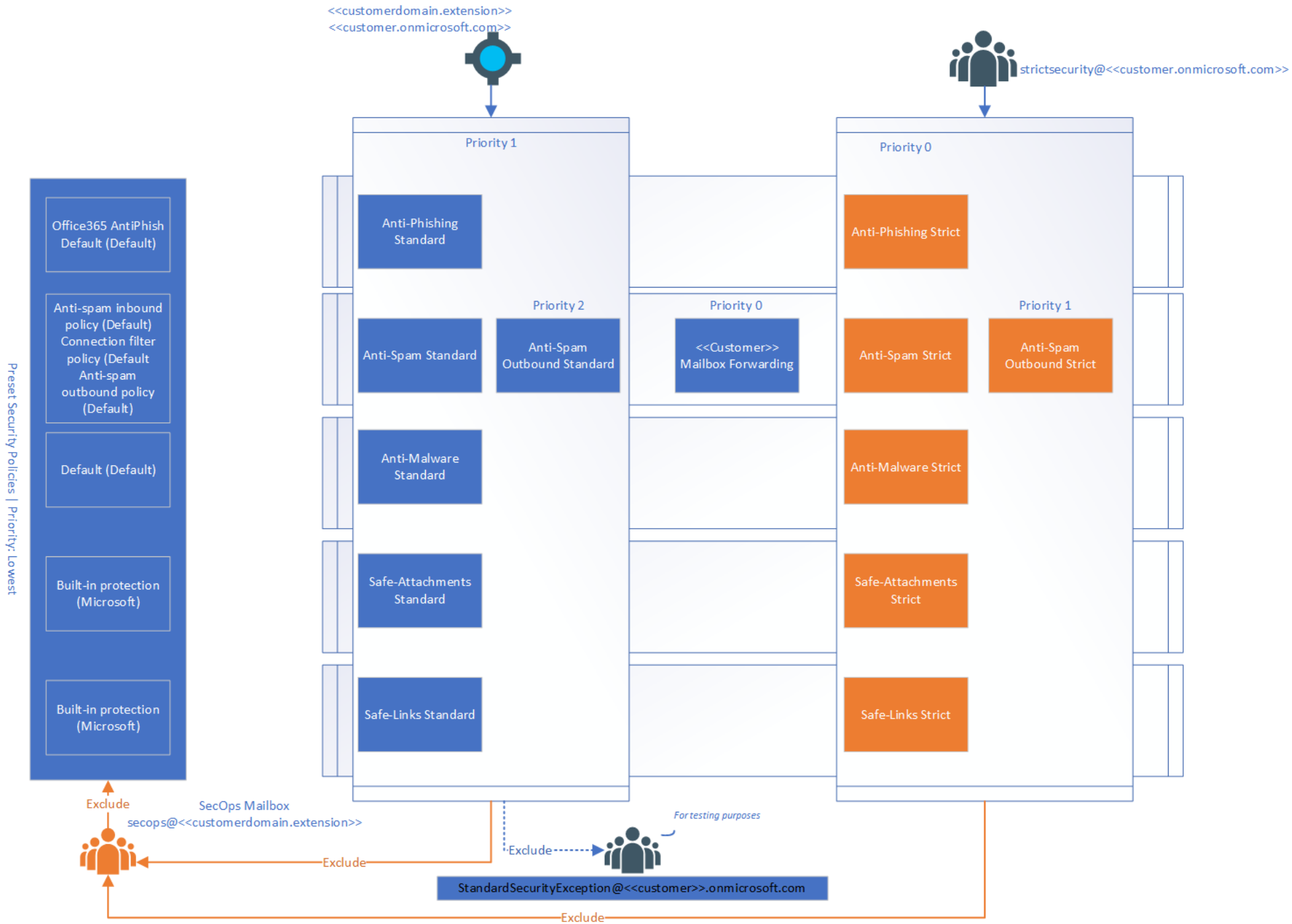
Standard recommendations | Strict recommendations | Configuration drift analysis and history

Anti-spam	Anti-phishing	Safe Links
3	21	7

Refresh

31 items | Search | Filter

Recommendations	Policy	Policy group/setting name	Policy type	Current configuration	Last modified	Status
Change 7 to 6	Default	Bulk email threshold	Anti-spam	7	8 Sep 2021 21:53	Not started
Change 15 to 30	Default	Quarantine retention period	Anti-spam	15	8 Sep 2021 21:53	Not started
Change 7 to 6	SaW - Anti Spam Standard - v1.11	Bulk email threshold	Anti-spam	7	8 Sep 2023 13:40	Not started
Change False to True	Office365 AntiPhish Default	Add users to protect	Anti-phishing	False	25 Oct 2020 12:41	Not started
Change False to True	Office365 AntiPhish Default	Automatically include the domains I own	Anti-phishing	False	25 Oct 2020 12:41	Not started
Change False to True	Office365 AntiPhish Default	Include custom domains	Anti-phishing	False	25 Oct 2020 12:41	Not started
Quarantine message	Office365 AntiPhish Default	If email is sent by an impersonated user	Anti-phishing	No action	25 Oct 2020 12:41	Not started
Quarantine message	Office365 AntiPhish Default	If email is sent by an impersonated domain	Anti-phishing	No action	25 Oct 2020 12:41	Not started
Change False to True	Office365 AntiPhish Default	Enable Intelligence for impersonation protectio...	Anti-phishing	False	25 Oct 2020 12:41	Not started
Change False to True	Office365 AntiPhish Default	Show tip for impersonated users	Anti-phishing	False	25 Oct 2020 12:41	Not started


<<customerdomain.extension>>
<<customer.onmicrosoft.com>>
strictsecurity@<<customer.onmicrosoft.com>>
Priority 1
Priority 0
Anti-Phishing Standard
Anti-Phishing Strict
Priority 2
Priority 0
Priority 1
Anti-Spam Standard
Anti-Spam Outbound Standard
<<Customer>> Mailbox Forwarding
Anti-Spam Strict
Anti-Spam Outbound Strict
Anti-Malware Standard
Anti-Malware Strict
Safe-Attachments Standard
Safe-Attachments Strict
Safe-Links Standard
Safe-Links Strict
Preset Security Policies | Priority: Lowest
Office365 AntiPhish Default (Default)
Anti-spam inbound policy (Default) Connection filter policy (Default Anti-spam outbound policy (Default)
Default (Default)
Built-in protection (Microsoft)
Built-in protection (Microsoft)
Exclude
SecOps Mailbox
secops@<<customerdomain.extension>>
Exclude
Exclude
For testing purposes
StandardSecurityException@<<customer>>.onmicrosoft.com
Exclude

Outgoing email

- Outbound SPAM policies
- Email Authentication

Requirements for all senders

Starting February 1, 2024, all senders who send email to Gmail accounts must meet the requirements in this section.

Important: If you send more than 5,000 messages per day to Gmail accounts, follow the Requirements for sending 5,000 or more messages per day.

- Set up SPF or DKIM email authentication for your domain.
- Ensure that sending domains or IPs have valid forward and reverse DNS records, also referred to as PTR records. Learn more
- Use a TLS connection for transmitting email. For steps to set up TLS in Google Workspace, visit Require a secure connection for email.
- Keep spam rates reported in Postmaster Tools below 0.10% and avoid ever reaching a spam rate of 0.30% or higher. Learn more about spam rates.
- Format messages according to the Internet Message Format standard (RFC 5322).
- Don't impersonate Gmail From: headers. Gmail will begin using a DMARC **quarantine** enforcement policy, and impersonating Gmail From: headers might impact your email delivery.
- If you regularly forward email, including using mailing lists or inbound gateways, add ARC headers to outgoing email. ARC headers indicate the message was forwarded and identify you as the forwarder. Mailing list senders should also add a List-id: header, which specifies the mailing list, to outgoing messages.

Requirements for sending 5,000 or more messages per day

Starting February 1, 2024, senders who send more than 5,000 messages per day to Gmail accounts must meet the requirements in this section.

- Set up SPF and DKIM email authentication for your domain.
- Ensure that sending domains or IPs have valid forward and reverse DNS records, also

Bulk email sending guidelines & tools

Email sender guidelines
Email sender guidelines FAQ
Feedback Loop
Postmaster Tools

Important: If you send more than 5,000 messages per day to Gmail accounts, follow the Requirements for sending 5,000 or more messages per day.

- Set up SPF or DKIM email authentication for your domain.
- Ensure that sending domains or IPs have valid forward and reverse DNS records, also referred to as PTR records. Learn more
- Use a TLS connection for transmitting email. For steps to set up TLS in Google Workspace, visit Require a secure connection for email.
- Keep spam rates reported in Postmaster Tools below 0.10% and avoid ever reaching a spam rate of 0.30% or higher. Learn more about spam rates.
- Format messages according to the Internet Message Format standard (RFC 5322).
- Don't impersonate Gmail From: headers. Gmail will begin using a DMARC **quarantine** enforcement policy, and impersonating Gmail From: headers might impact your email delivery.
- If you regularly forward email, including using mailing lists or inbound gateways, add ARC headers to outgoing email. ARC headers indicate the message was forwarded and identify you as the forwarder. Mailing list senders should also add a List-id: header, which specifies the mailing list, to outgoing messages.

Email Authentication

DKIM SPF DMARC

Email authentication/validation

- Sender Policy Framework (SPF)
  - How Sender Policy Framework (SPF) prevents spoofing | Microsoft Learn
- Domain-based Message Authentication, Reporting & Conformance (DMARC)
  - Set DMARC policy for parked domains
- DomainKeys Identified Mail (DKIM)

DEMO

SPF, DKIM and DMARC

EUROPEAN
MCT SUMMIT 2024
THE NETHERLANDS

Manage

Security Operations Guide for Defender for Office 365 | Microsoft Learn: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-sec-ops-guide?view=o365-worldwide

Daily, weekly, monthly tasks related to managing EOP and MDO

GRACIAS

EUROPEAN
MCT SUMMIT 2024

THE NETHERLANDS

Por estar aqui y reir