softwareone

Transformation. All in one.

Microsoft Security NL - Navigating Exchange Online: A Comprehensive Look at Transport Mechanisms
February 11th, 2025

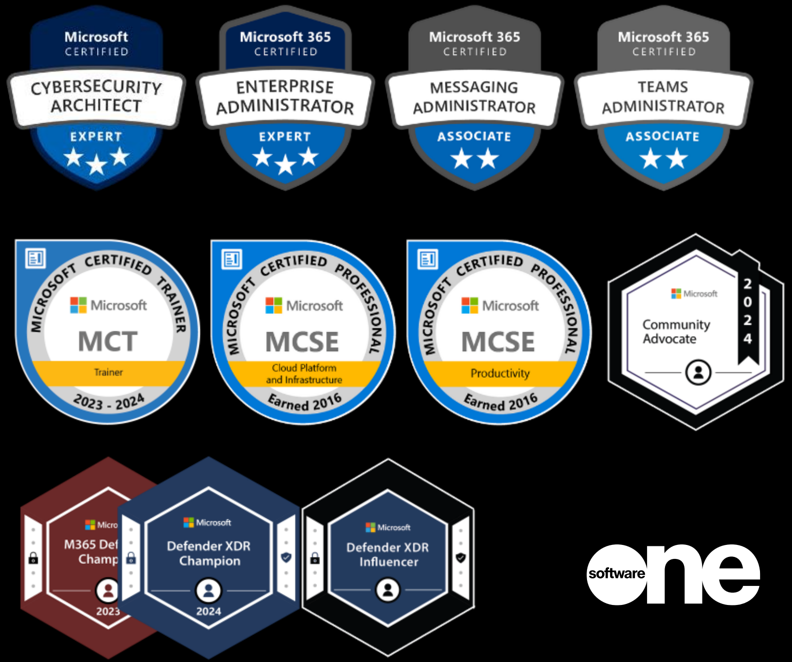
softwareone step ahead.

Erik Stiphout

Sr. Consultant Digital Workplace

✉ :

☎ :


Microsoft CERTIFIED CYBERSECURITY ARCHITECT EXPERT
Microsoft 365 CERTIFIED ENTERPRISE ADMINISTRATOR EXPERT
Microsoft 365 CERTIFIED MESSAGING ADMINISTRATOR ASSOCIATE
Microsoft 365 CERTIFIED TEAMS ADMINISTRATOR ASSOCIATE
MICROSOFT CERTIFIED TRAINER Microsoft MCT Trainer 2023 - 2024
MICROSOFT CERTIFIED PROFESSIONAL Microsoft MCSE Cloud Platform and Infrastructure Earned 2016
MICROSOFT CERTIFIED PROFESSIONAL Microsoft MCSE Productivity Earned 2016
Microsoft Community Advocate 2024
Micro M365 Def Champ 2023
Microsoft Defender XDR Champion 2024
Microsoft Defender XDR Influencer

softwareone

Lets talk about Microsoft and Email Security
Lets go, in and out.
quick 20 minute adventure

01 Basic rules of secure email transport

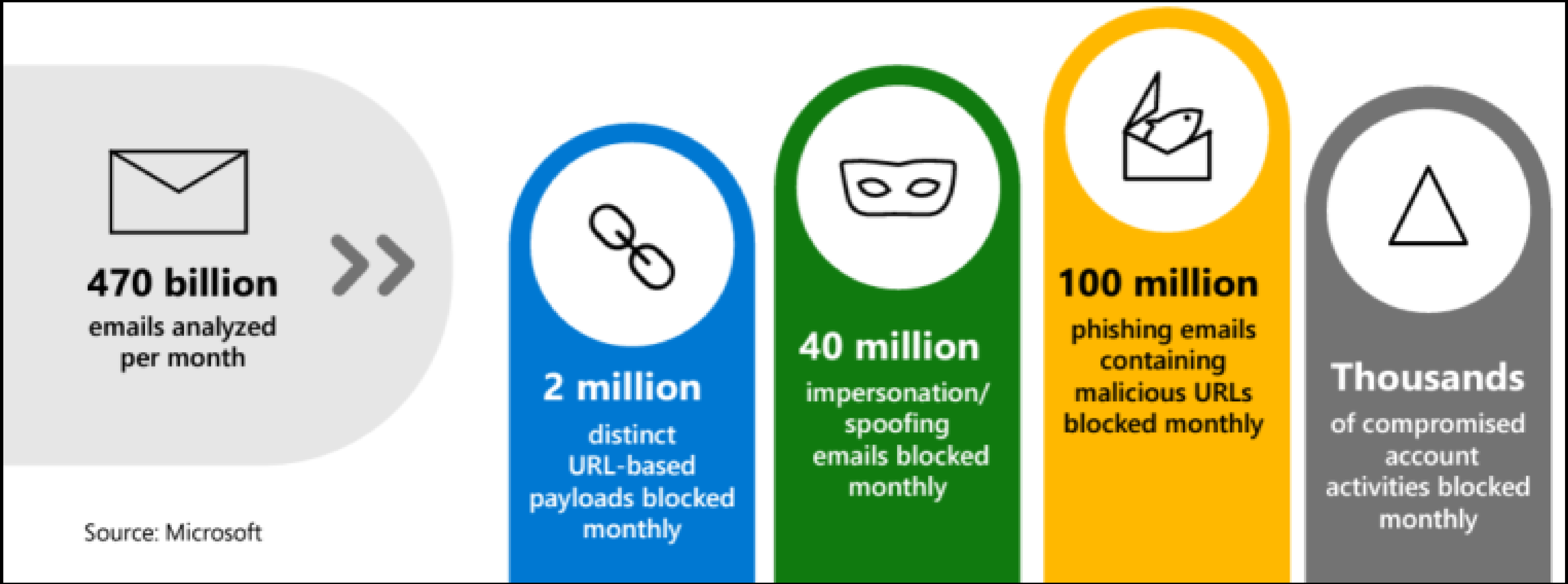
02 Security settings in EXO & EOP

03 Advanced configuration of EXO & EOP

04 Q & A

Basic rules of secure email transport

E-mail by the numbers (as of august 2024)



470 billion emails analyzed per month

2 million distinct URL-based payloads blocked monthly

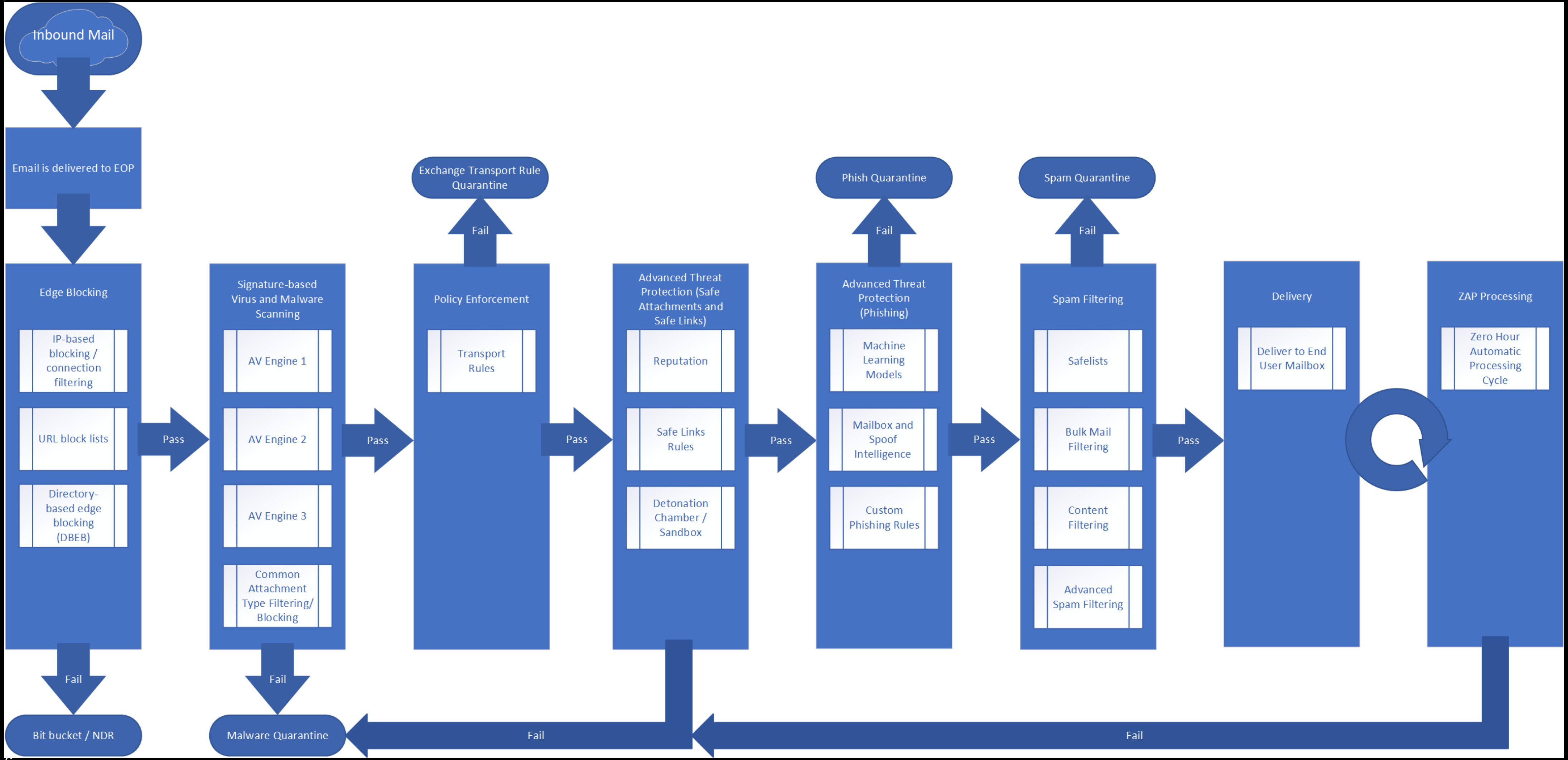
40 million impersonation/ spoofing emails blocked monthly

100 million phishing emails containing malicious URLs blocked monthly

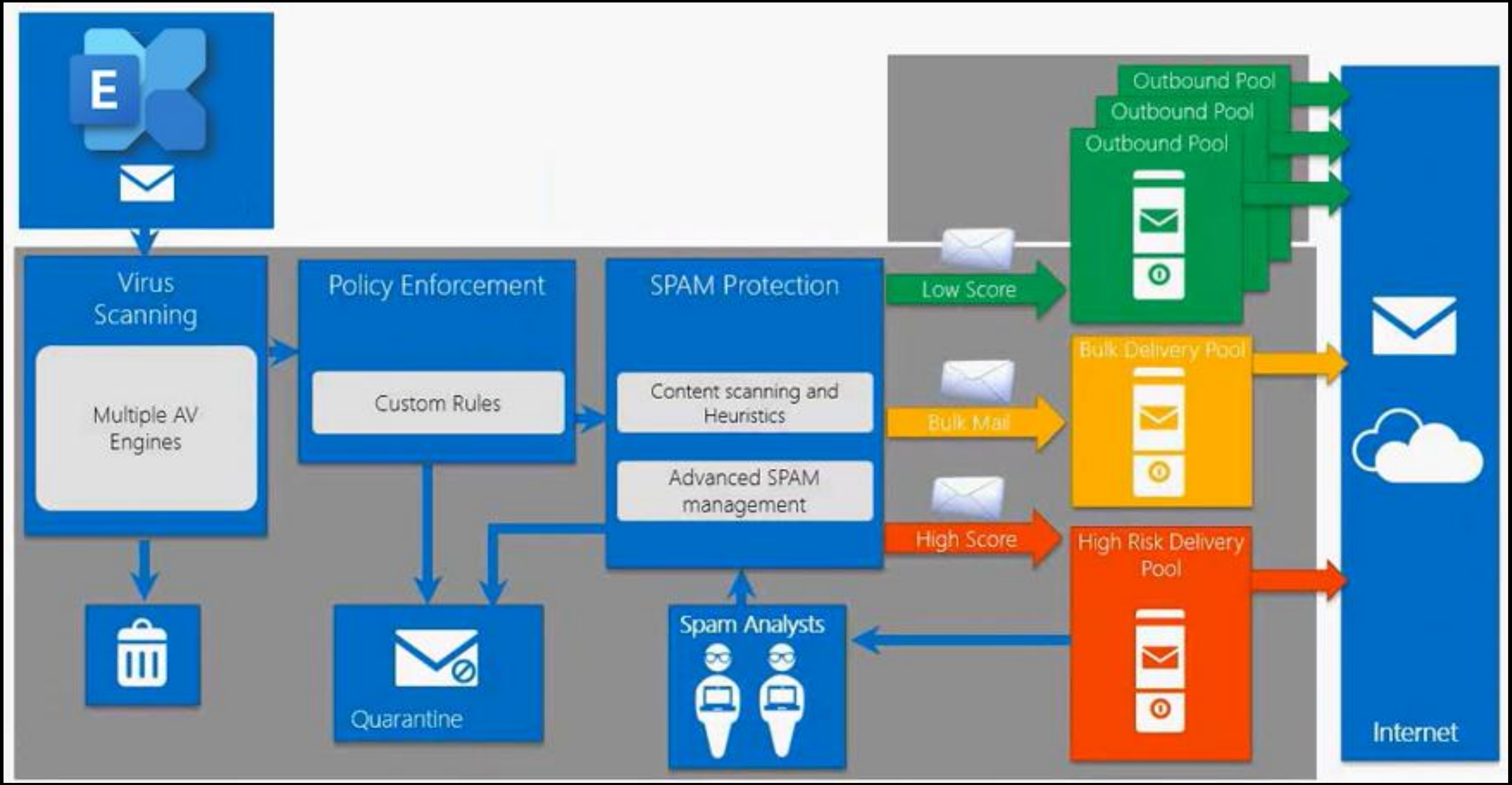
Thousands of compromised account activities blocked monthly

Source: Microsoft

EOP & EXO inbound flow


Inbound Mail
Email is delivered to EOP
Edge Blocking
IP-based blocking / connection filtering
URL block lists
Directory-based edge blocking (DBEB)
Fail
Bit bucket / NDR
Pass
Signature-based Virus and Malware Scanning
AV Engine 1
AV Engine 2
AV Engine 3
Common Attachment Type Filtering/ Blocking
Fail
Malware Quarantine
Pass
Exchange Transport Rule Quarantine
Fail
Policy Enforcement
Transport Rules
Pass
Advanced Threat Protection (Safe Attachments and Safe Links)
Reputation
Safe Links Rules
Detonation Chamber / Sandbox
Fail
Pass
Phish Quarantine
Fail
Advanced Threat Protection (Phishing)
Machine Learning Models
Mailbox and Spoof Intelligence
Custom Phishing Rules
Pass
Spam Quarantine
Fail
Spam Filtering
Safelists
Bulk Mail Filtering
Content Filtering
Advanced Spam Filtering
Pass
Delivery
Deliver to End User Mailbox
ZAP Processing
Zero Hour Automatic Processing Cycle
Fail

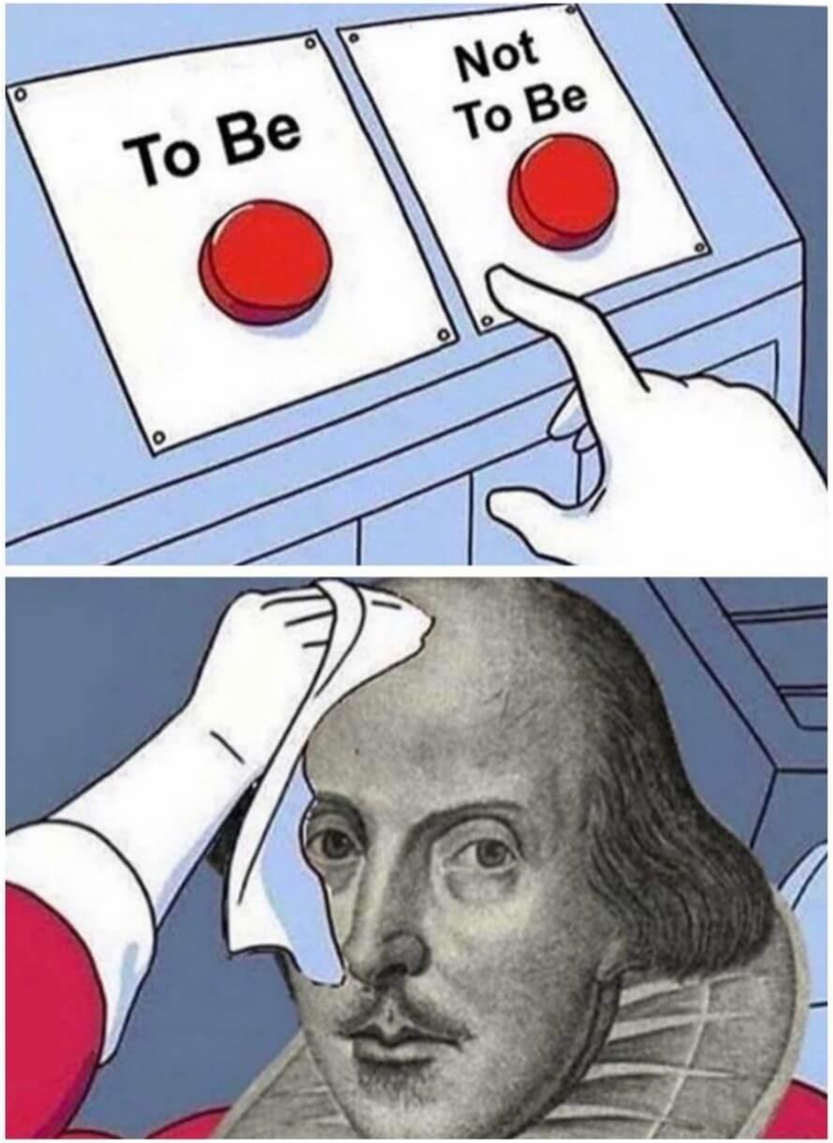
EOP & EXO outbound flow



To MX or not to MX

Should you point your MX to Microsoft?

- Yes…
- Really, yes….
- Maybe...
- Obviously, the discussion on what is best for each organization individually can be debated endlessly but:
  - Microsoft has access to the entirety of the mail stack
  - MDO does it's magic generally inline making it multi client
  - Agentless protection makes MDO very light touch
- Except when you need….
  - Auto-responders
  - Mass-email pointed at external recipients
  - Backup or compliance archiving



The M365 tenant and your domains

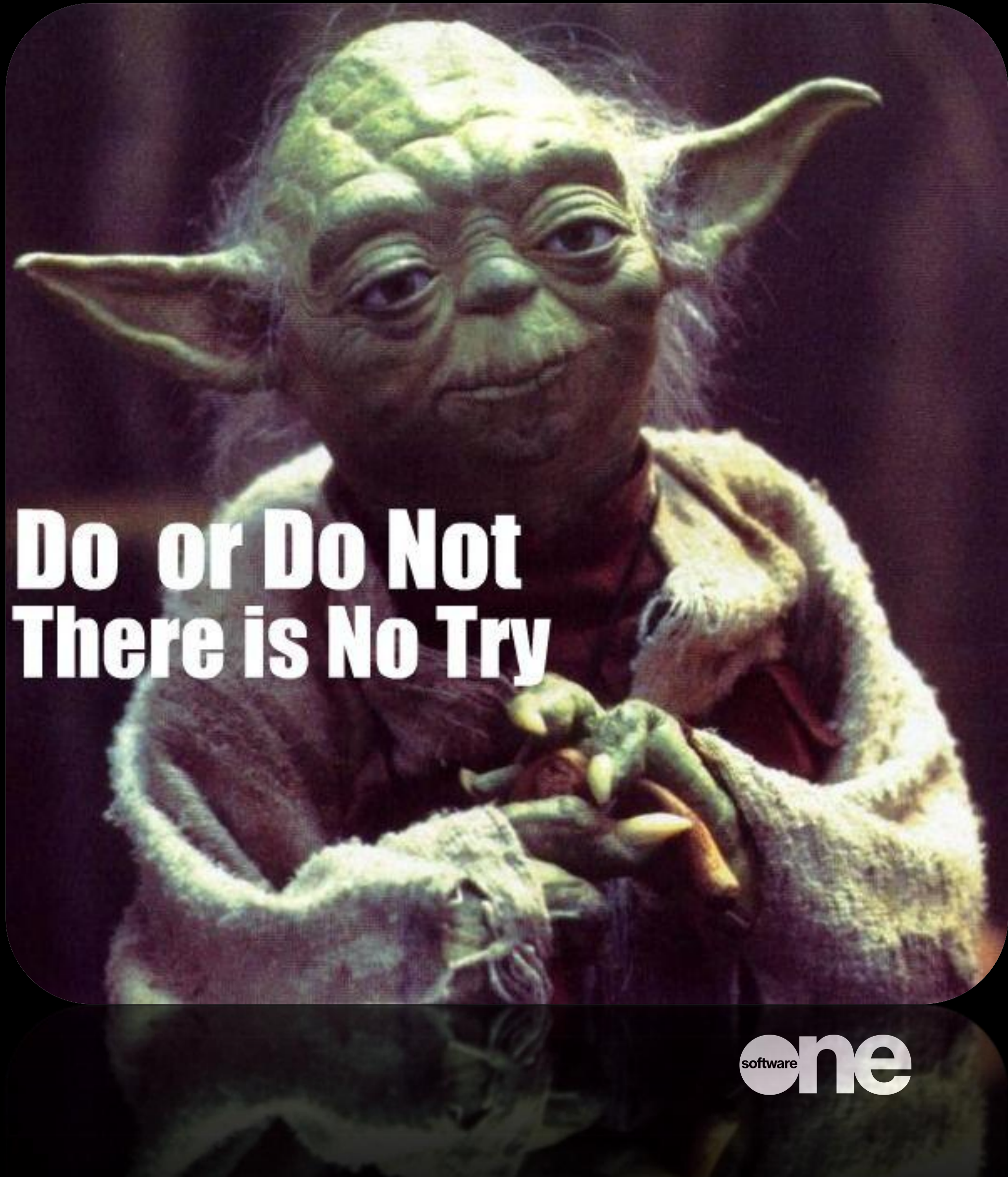
Adding all your domains in ownership

- Your organization may own a lot of domains so familiarize yourself with bulk adding of domains and the verification process.
- A good DNS registar will allow you to set a template which would automate the administration of new domains to secure them further.
- When a domain is added to the M365 tenant and ownership is proven, Microsoft will add “protection” to it or at least know not to allow it through as a sender domain.

Do or do not there is no try

Hardening all your domains

- First, the domains that do not receive or send e-mail actively.
  - SPF
  - DMARC
  - MX (rfc7505)
  - MTA – STS (rfc8461)
- So why not DKIM or DANE?
- And what about sub-domains?



Do or do not there is no try

Hardening all your domains

- Second, the domains that do receive or send e-mail actively.

- SPF

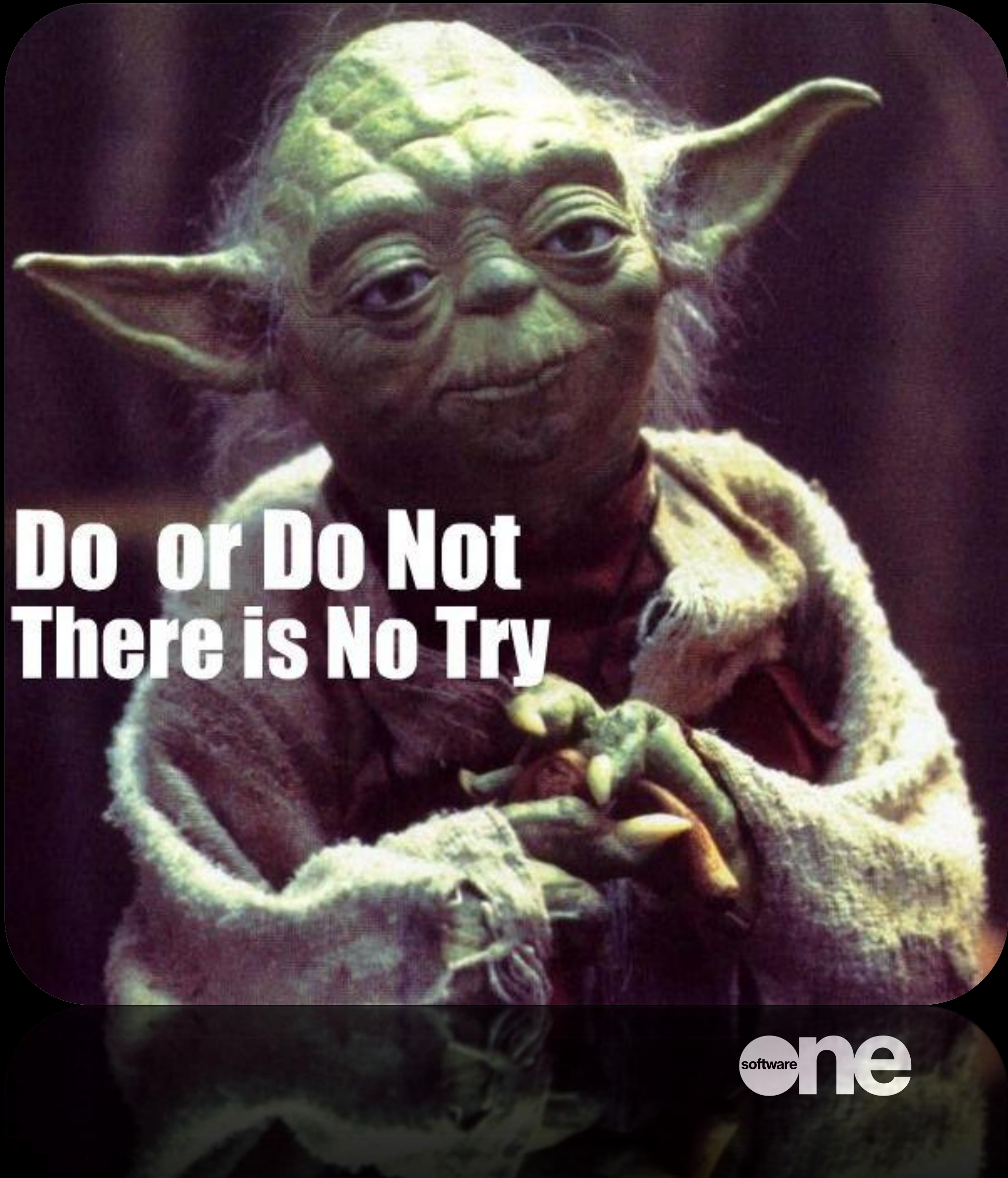
```
v=spf1 ip4:192.168.0.10 ip4:192.168.0.12
include:spf.protection.outlook.com -all
```

- DKIM

```
selector1._domainkey
selector1-contoso-
com._domainkey.contoso.onmicrosoft.com.
```

- DMARC

```
v=DMARC1; p=reject; sp=reject;
rua=mailto:rua@contoso.com;
ruf=mailto:ruf@contoso.com; aspf=r; adkim=r;
ri=86400; fo=1:d:s
```



(Controversial) Opinion time

How to handle sharing e-mail domains with partners

- The root domain is “sacred” and no one should use it but your own MTA(s).
- Partners & vendors should use subdomains (yours or theirs)
  - More room in the SPF record
  - Separate routing of email

```
mail.external.vendor.contoso.com
               or
      mail.contoso.vendor.com
```

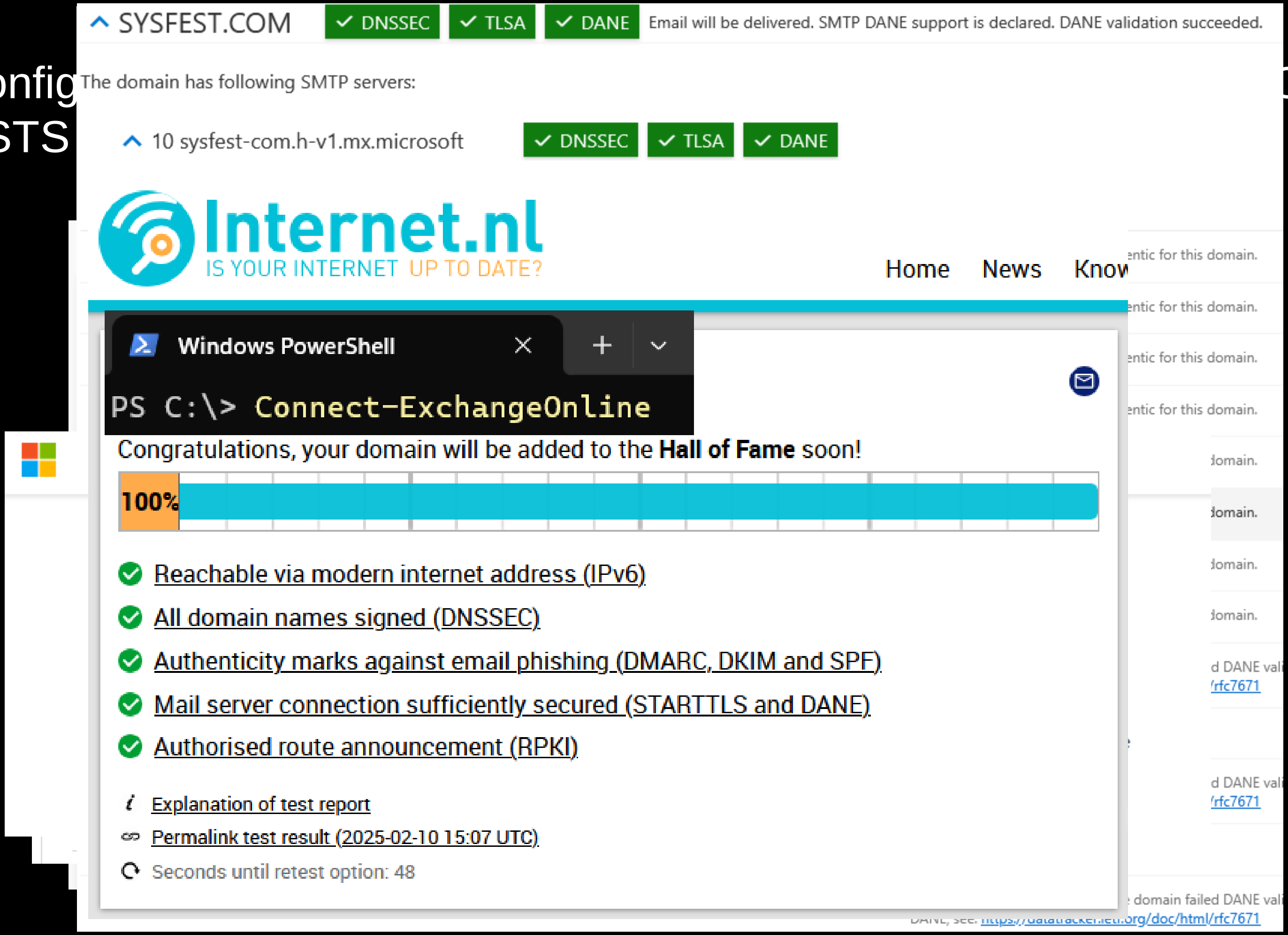
Setting up more e-mail security protocols

Choosing what works for you

- DANE (& DNSSEC)
- MTA-STS (& TLS-RPT)
- BIMI (pronounced: Bih-mee)
- ARC Seal
  - SPF fails because of the new message source (IP address).
  - DKIM fails because of content modification.
  - DMARC fails because of the SPF and DKIM failures.

Let’s quickly setup inbound DANE

- NB. If you have config D NOT FORGET to change the MTA-STS



SYSFEST.COM ✓ DNSSEC ✓ TLSA ✓ DANE Email will be delivered. SMTP DANE support is declared. DANE validation succeeded.

The domain has following SMTP servers:

10 sysfest-com.h-v1.mx.microsoft ✓ DNSSEC ✓ TLSA ✓ DANE

```
PS C:\> Connect-ExchangeOnline
```

Congratulations, your domain will be added to the **Hall of Fame** soon!

100%

- ✓ Reachable via modern internet address (IPv6)
- ✓ All domain names signed (DNSSEC)
- ✓ Authenticity marks against email phishing (DMARC, DKIM and SPF)
- ✓ Mail server connection sufficiently secured (STARTTLS and DANE)
- ✓ Authorised route announcement (RPKI)

Explanation of test report

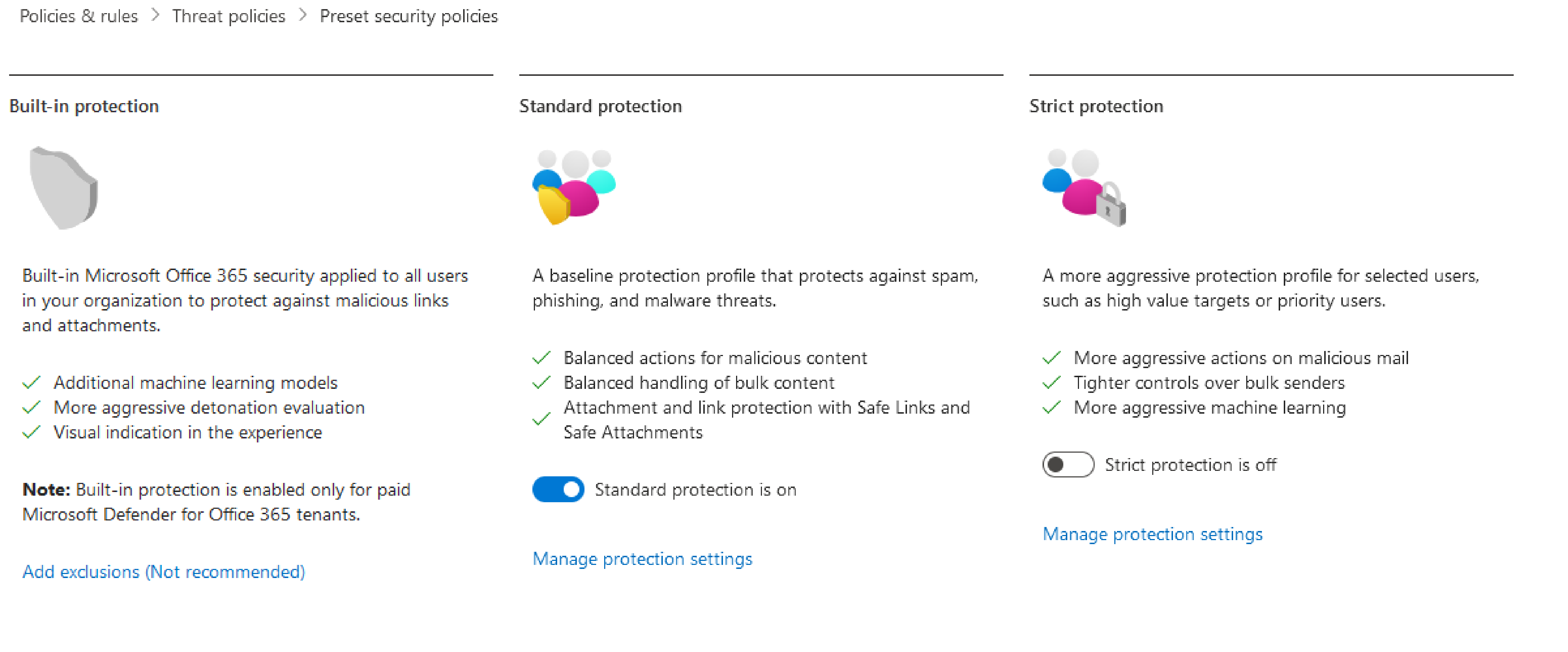
Permalink test result (2025-02-10 15:07 UTC)

Seconds until retest option: 48

Security settings in EXO & EOP

Utilize the Microsoft pre-set policies or build your own

Would you or wouldn't you.



Policies & rules > Threat policies > Preset security policies

Built-in protection

Built-in Microsoft Office 365 security applied to all users in your organization to protect against malicious links and attachments.

- ✓ Additional machine learning models
- ✓ More aggressive detonation evaluation
- ✓ Visual indication in the experience

Note: Built-in protection is enabled only for paid Microsoft Defender for Office 365 tenants.

Add exclusions (Not recommended)

Standard protection

A baseline protection profile that protects against spam, phishing, and malware threats.

- ✓ Balanced actions for malicious content
- ✓ Balanced handling of bulk content
- ✓ Attachment and link protection with Safe Links and Safe Attachments

Standard protection is on

Manage protection settings

Strict protection

A more aggressive protection profile for selected users, such as high value targets or priority users.

- ✓ More aggressive actions on malicious mail
- ✓ Tighter controls over bulk senders
- ✓ More aggressive machine learning

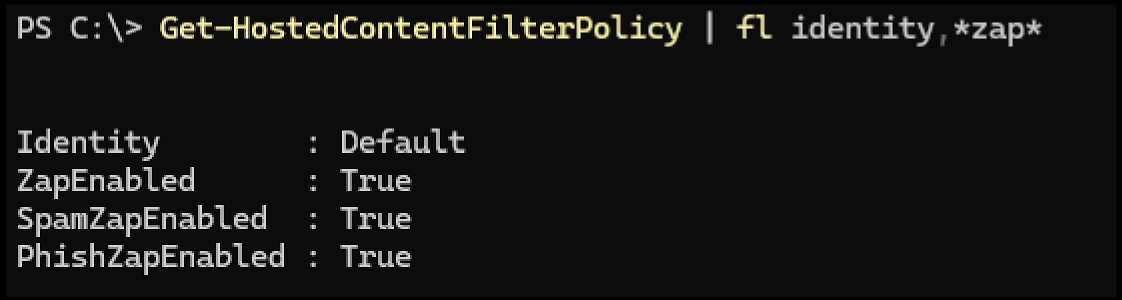
Strict protection is off

Manage protection settings

Zero-hour Auto Purge (ZAP)

Best feature included with Exchange Online

- There is no ZAP for EOP standalone
- Explorer only lists ZAP with MDO P2 or M365 E5



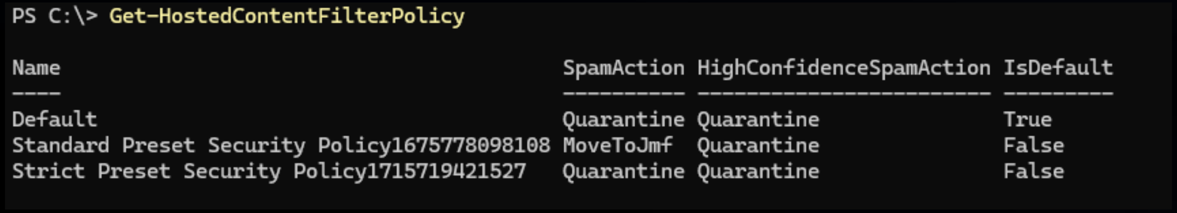
```
PS C:\> Get-HostedContentFilterPolicy | fl identity,*zap*


Identity        : Default
ZapEnabled      : True
SpamZapEnabled  : True
PhishZapEnabled : True
```

Putting e-mail in quarantine and not telling anyone

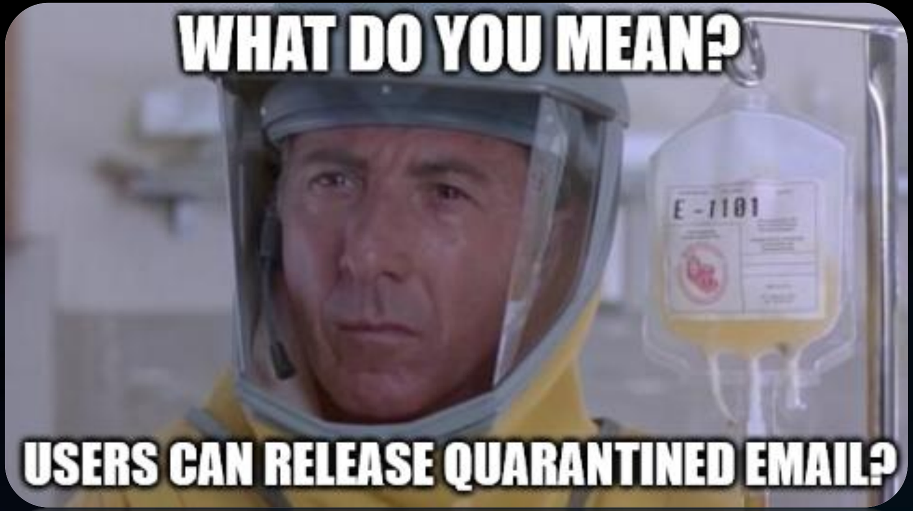
Why no one should allow release of email but you

- Quarantine policies



```
PS C:\> Get-HostedContentFilterPolicy

Name                                        SpamAction HighConfidenceSpamAction IsDefault
----                                        ---------- ------------------------ ---------
Default                                     Quarantine Quarantine               True
Standard Preset Security Policy1675778098108 MoveToJmf  Quarantine               False
Strict Preset Security Policy1715719421527   Quarantine Quarantine               False
```



My preferred common attachment filter

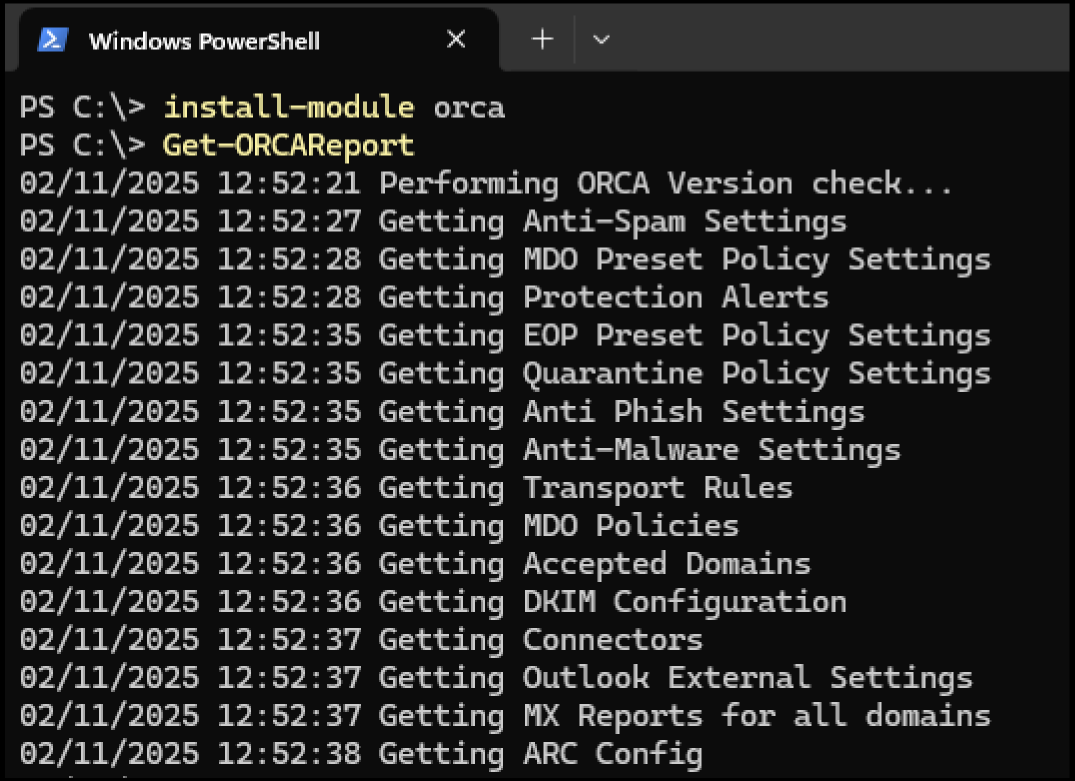
Block file extensions

- Default file types:
  - ace, ani, apk, app, appx, arj, bat, cab, cmd, com, deb, dex, dll, docm, elf, exe, hta, htm, html, img, iso, jar, jnlp, kext, lha, lib, library, link, lzh, macho, msc, msi, msix, msp, mst, pif, ppa, ppam, reg, rev, scf, scr, sct, sys, uif, vb, vbe, vbs, vxd, wsc, wsf, wsh, xll, xz, z
- Additional file types manually added
  - 7z, 7zip, a, accdb, accde, action, ade, adp, appxbundle, asf, asp, aspx, avi, bas, bin, bundle, bz, bz2, bzip2, caction, cer, chm, command, cpl, crt, csh, css, der, dgz, dmg, doc, docx, dos, dot, dotm, dtox [sic], dylib, font, fxp, gadget, gz, gzip, hlp, Hta, htm, html, imp, inf, ins, ipa, isp, its, js, jse, ksh, Lnk, lqy, mad, maf, mag, mam, maq, mar, mas, mat, mau, mav, maw, mda, mdb, mde, mdt, mdw, mdz, mht, mhtml, mscompress, msh, msh1, msh1xml, msh2, msh2xml, mshxml, msixbundle, o, obj, odp, ods, odt, one, onenote, ops, os2, package, pages, pbix, pcd, pdb, pdf, php, pkg, plg, plugin, pps, ppsm, ppsx, ppt, pptm, pptx, prf, prg, ps1, ps1xml, ps2, ps2xml, psc1, psc2, pst, pub, py, rar, rpm, rtf, scpt, service, sh, shb, shs, shtm, shx, so, tar, tarz, terminal, tgz, tmp, tool, url, vhd, vsd, vsdm, vsdx, vsmacros, vss, vssx, vst, vstm, vstx, vsw, w16, workflow, ws, xhtml, xla, xlam, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xnk, zi, zip, zipx.

Dude how's my MDO configuration?

Defender for Office 365 Recommended Configuration Analyzer (ORCA)

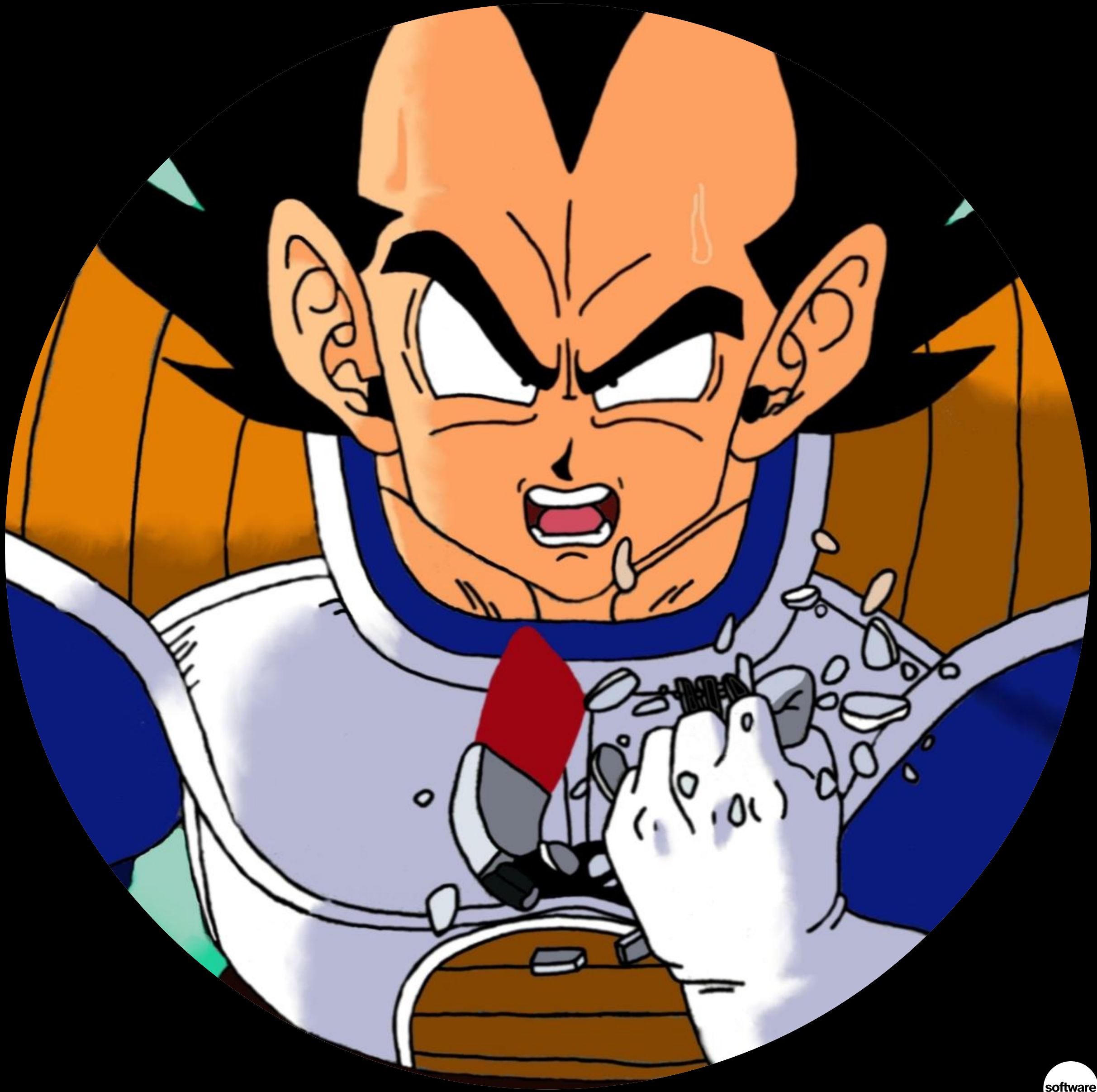
- https://github.com/cammurray/orca



```
PS C:\> install-module orca
PS C:\> Get-ORCAReport
02/11/2025 12:52:21 Performing ORCA Version check...
02/11/2025 12:52:27 Getting Anti-Spam Settings
02/11/2025 12:52:28 Getting MDO Preset Policy Settings
02/11/2025 12:52:28 Getting Protection Alerts
02/11/2025 12:52:35 Getting EOP Preset Policy Settings
02/11/2025 12:52:35 Getting Quarantine Policy Settings
02/11/2025 12:52:35 Getting Anti Phish Settings
02/11/2025 12:52:35 Getting Anti-Malware Settings
02/11/2025 12:52:36 Getting Transport Rules
02/11/2025 12:52:36 Getting MDO Policies
02/11/2025 12:52:36 Getting Accepted Domains
02/11/2025 12:52:36 Getting DKIM Configuration
02/11/2025 12:52:37 Getting Connectors
02/11/2025 12:52:37 Getting Outlook External Settings
02/11/2025 12:52:37 Getting MX Reports for all domains
02/11/2025 12:52:38 Getting ARC Config
```

I DONT KNOW WHAT CONFIGURATION TO CHANGE
AND AT THIS POINT I'M TOO AFRAID TO ASK

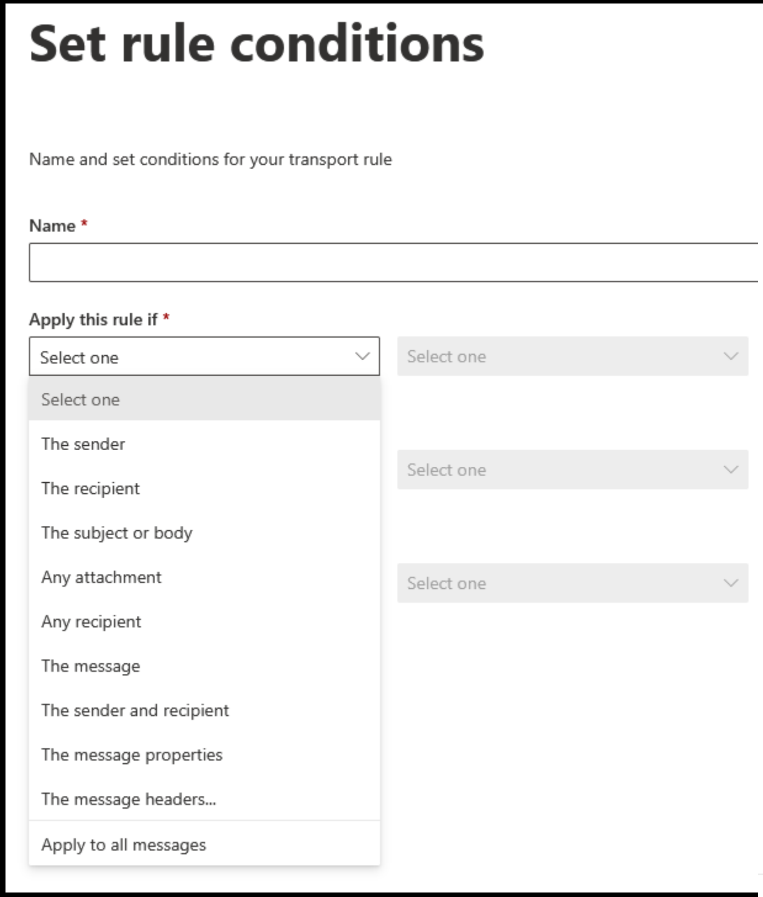
Advanced configuration of EXO & EOP



Mail flow rules (aka Transport rules)

Outlook inbox rules on steroids

- Email addressing management
- Flow management
- Safe senders (accept DKIM/DMARC)
- Suwi mail
- Signature tools (Exclaimer / Codetwo)
- Other solutions



Set rule conditions

Name and set conditions for your transport rule

Name *

Apply this rule if *

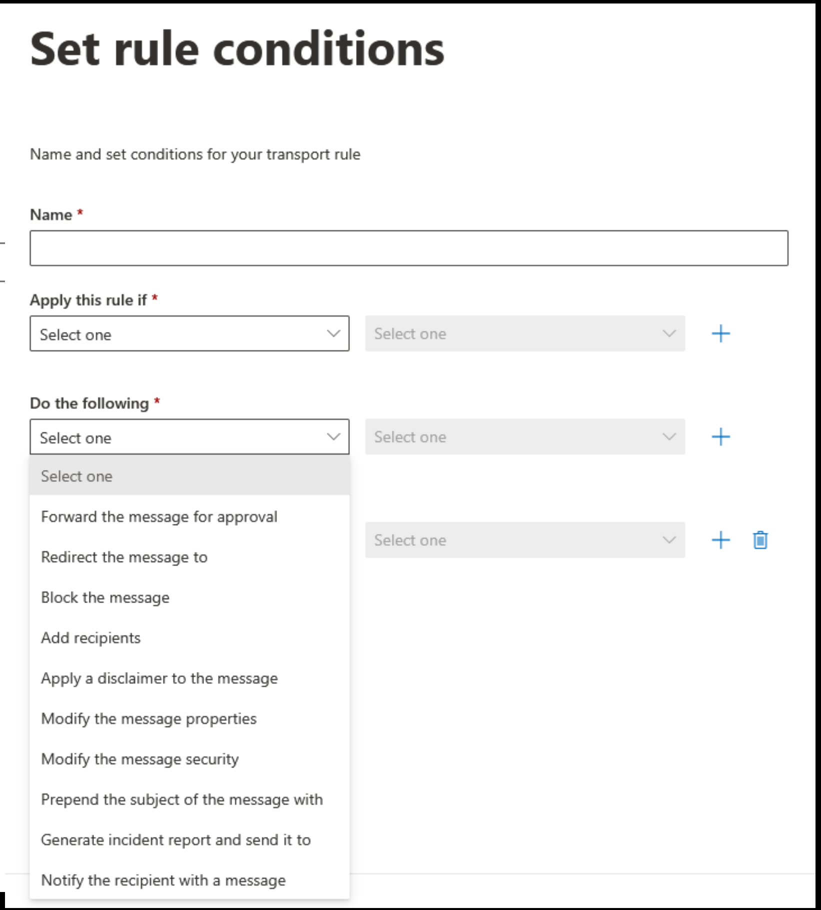
Select one

- Select one
- The sender
- The recipient
- The subject or body
- Any attachment
- Any recipient
- The message
- The sender and recipient
- The message properties
- The message headers...
- Apply to all messages

Select one

Select one

Select one



Set rule conditions

Name and set conditions for your transport rule

Name *

Apply this rule if *

Select one

Select one

Do the following *

Select one

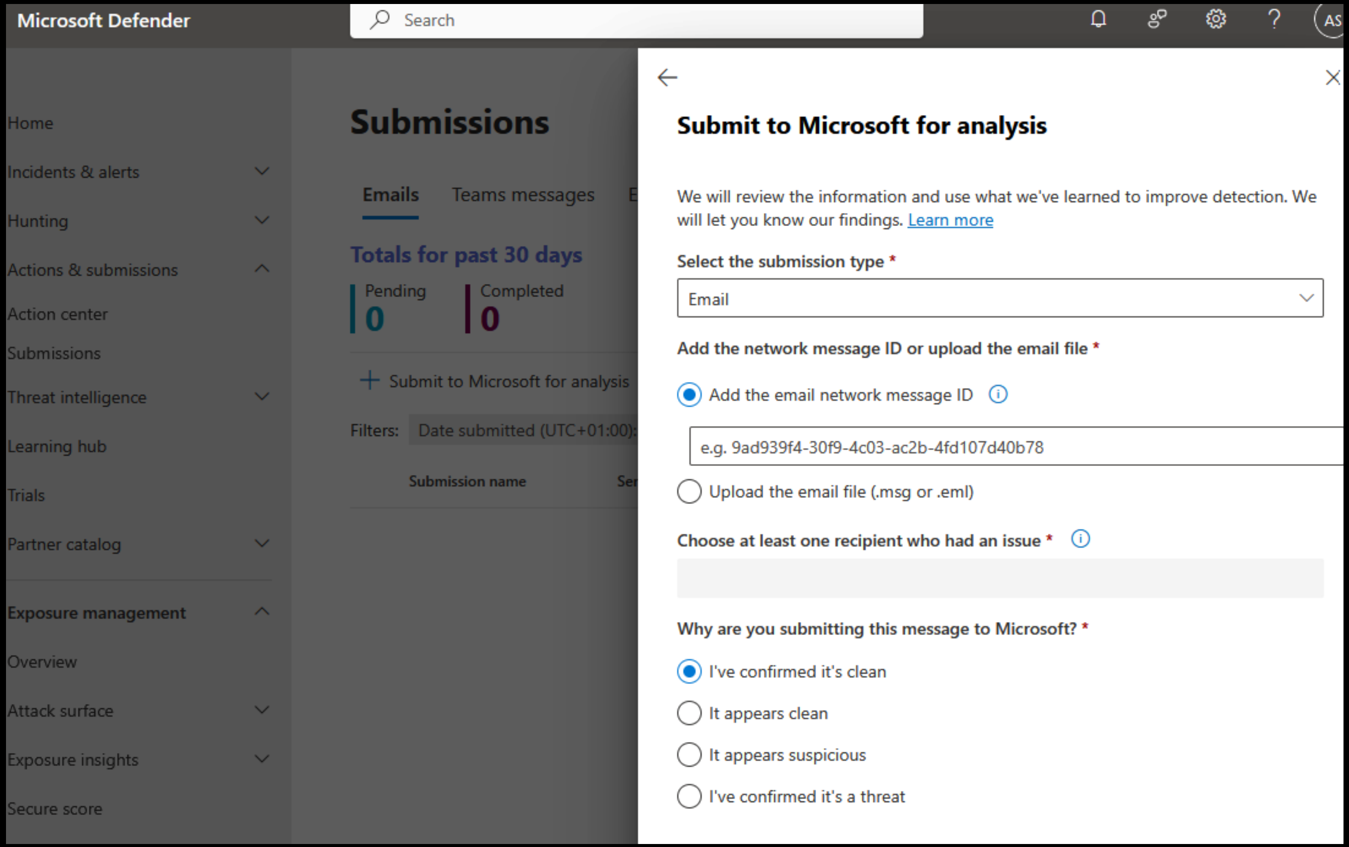
- Select one
- Forward the message for approval
- Redirect the message to
- Block the message
- Add recipients
- Apply a disclaimer to the message
- Modify the message properties
- Modify the message security
- Prepend the subject of the message with
- Generate incident report and send it to
- Notify the recipient with a message

Select one

Select one

Tenant Allow & Block lists

Why not every false positive is worth acting on



Submit to Microsoft for analysis

We will review the information and use what we've learned to improve detection. We will let you know our findings. Learn more

Select the submission type *

Email

Add the network message ID or upload the email file *

● Add the email network message ID

e.g. 9ad939f4-30f9-4c03-ac2b-4fd107d40b78

○ Upload the email file (.msg or .eml)

Choose at least one recipient who had an issue *

Why are you submitting this message to Microsoft? *

● I've confirmed it's clean

○ It appears clean

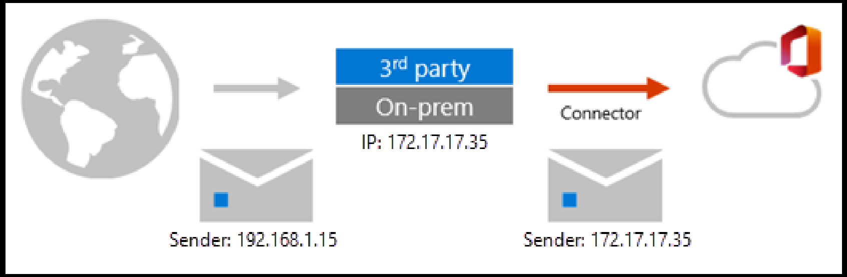
○ It appears suspicious

○ I've confirmed it's a threat

Enhanced filtering for your connectors

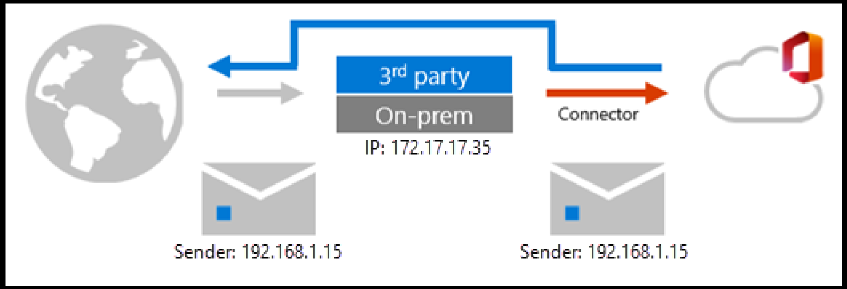
If you have a 3rd party email filter or pass all email through your hybrid server first

- Reduced false positives in DMARC from content modification and lack of an ARC seal.
- Makes AIR more reliable
- Better reputation verification (SPF/DKIM/DMARC)



Use enhance filtering with:

- Third-party cloud filtering services
- Managed filtering appliances
- Hybrid environments (for example, on-premises Exchange)



Sender rewriting Scheme & Cross tenant SMTP domain sharing

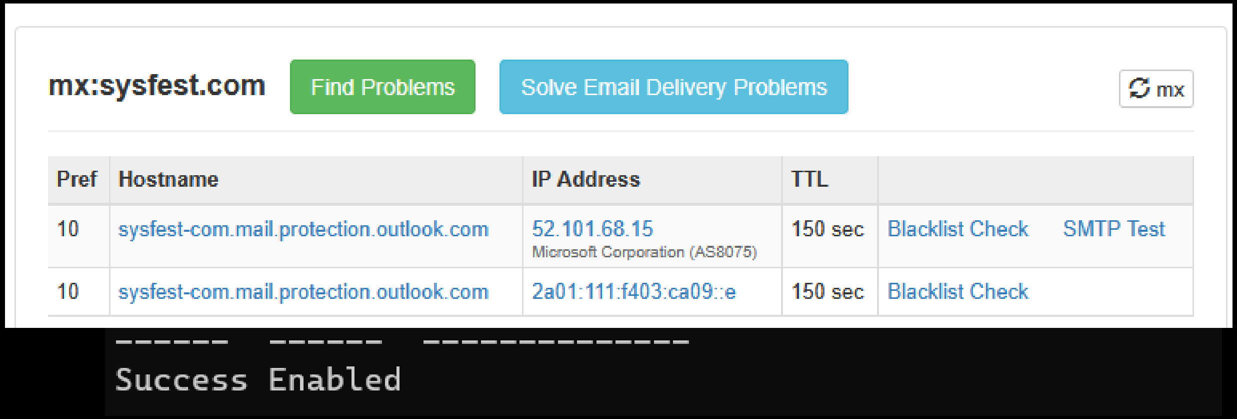
Fun with features no one has heard of.

- The Sender Rewriting Scheme (SRS) functionality was added to resolve a problem in which auto forwarding was incompatible with SPF. The SRS feature rewrites the P1 From address (also known as the Envelope From address) for all applicable messages that are sent externally
- Cross tenant SMTP domain sharing, (not to be confused with cross-tenant mailbox migration) still exists as a private preview although its development seems to have halted.

Manually enabling IPv6 in Exchange Online

Check to see if Microsoft has enabled your accepted domain(s) for IPv6

- Exchange Transport Rules or Data Loss Prevention policies which rely on the SenderIPRanges are a reason to opt out all accepted domains from IPv6.



Pref	Hostname	IP Address	TTL	
10	sysfest-com.mail.protection.outlook.com	52.101.68.15 Microsoft Corporation (AS8075)	150 sec	Blacklist Check SMTP Test
10	sysfest-com.mail.protection.outlook.com	2a01:111:f403:ca09::e	150 sec	Blacklist Check

```
-------  -------  ----------------
Success  Enabled
```

What's left on-premises that sends email?

Transitioning away from on-premises e-mail senders

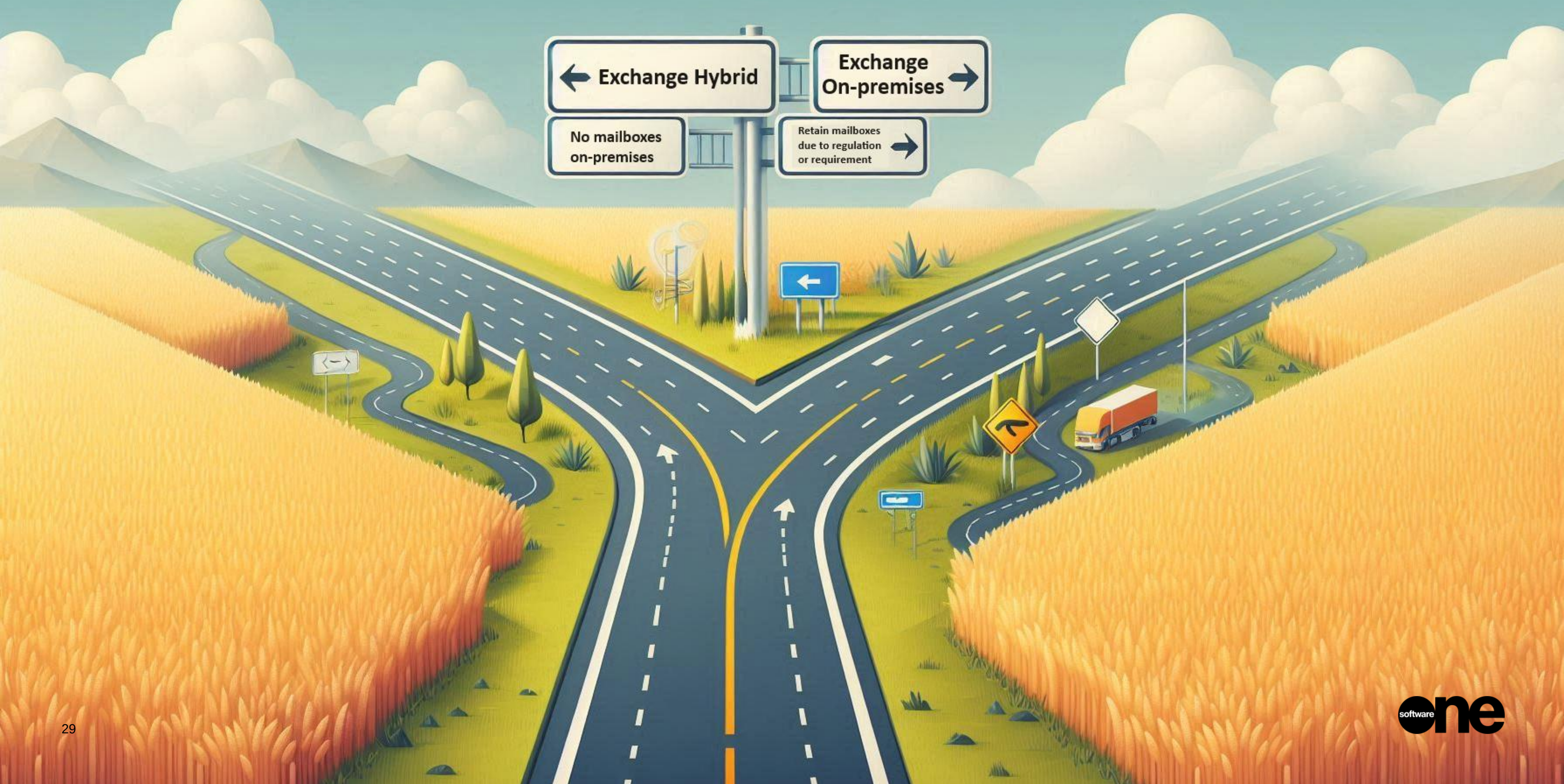
- **SMTP AUTH** **(EOL Sept 2025)**
- **Direct send**
- **SMTP relay**
- **Hybrid Exchange (or other MTA)**

Transport Enforcement System in Exchange Online

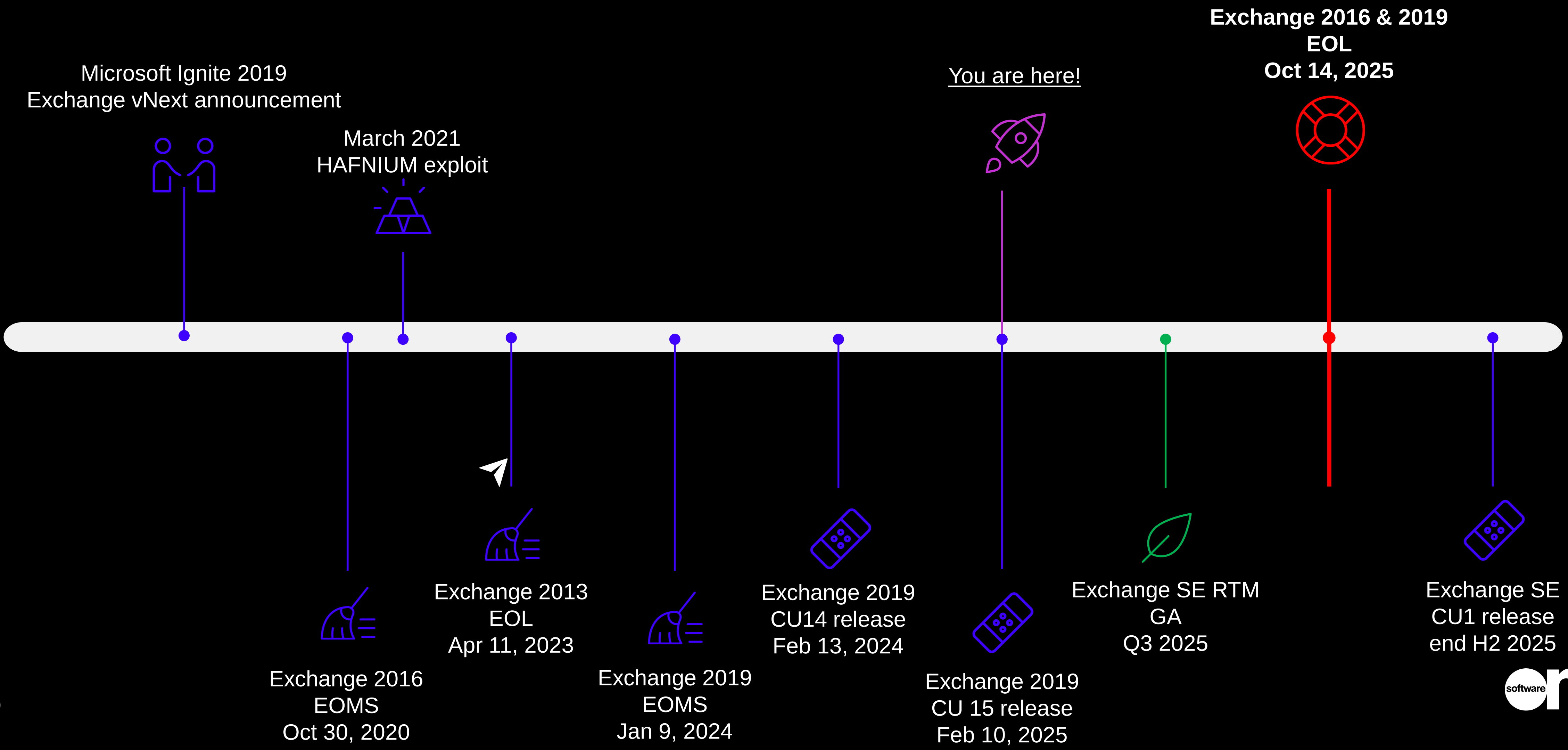
If your server updates areout-of-date Microsoft will block you.

- Expect Exchange Hybrid servers to be marked non-compliant if they are not kept updated (n-1) within 90 days.
- The measure is aimed at stopping compromised Exchange Servers (on-premises) being misused in the e-mail flow due to being unpatched or unsupported.

The fork in the road for customers using Exchange Server today



Exchange Server (on-premises) Replacement Roadmap



Microsoft Ignite 2019
Exchange vNext announcement

Exchange 2016
EOMS
Oct 30, 2020

March 2021
HAFNIUM exploit

Exchange 2013
EOL
Apr 11, 2023

Exchange 2019
EOMS
Jan 9, 2024

Exchange 2019
CU14 release
Feb 13, 2024

You are here!

Exchange 2019
CU 15 release
Feb 10, 2025

Exchange SE RTM
GA
Q3 2025

Exchange 2016 & 2019
EOL
Oct 14, 2025

Exchange SE
CU1 release
end H2 2025

Wrapping up

- Configure all your domains in ownership and review your SPF, DKIM and DMARC settings for them.
- Enable DNSSEC/DANE inbound and IPv6 for your inbound e-mail flow.
- Review all your security settings regularly and enhance where possible.
- Review your transport rules and don’t over complicate it if you don’t need to.
- Evaluate the Allow list every 60 days.
- Don’t forget to upgrade your on-prem environment to Exchange SE before October 2025 to stay secure.

Thank you for your attention!

Any questions?

Let's connect!

LinkedIn:
www.linkedin.com/in/erikstiphout

X:
x.com/erikstip

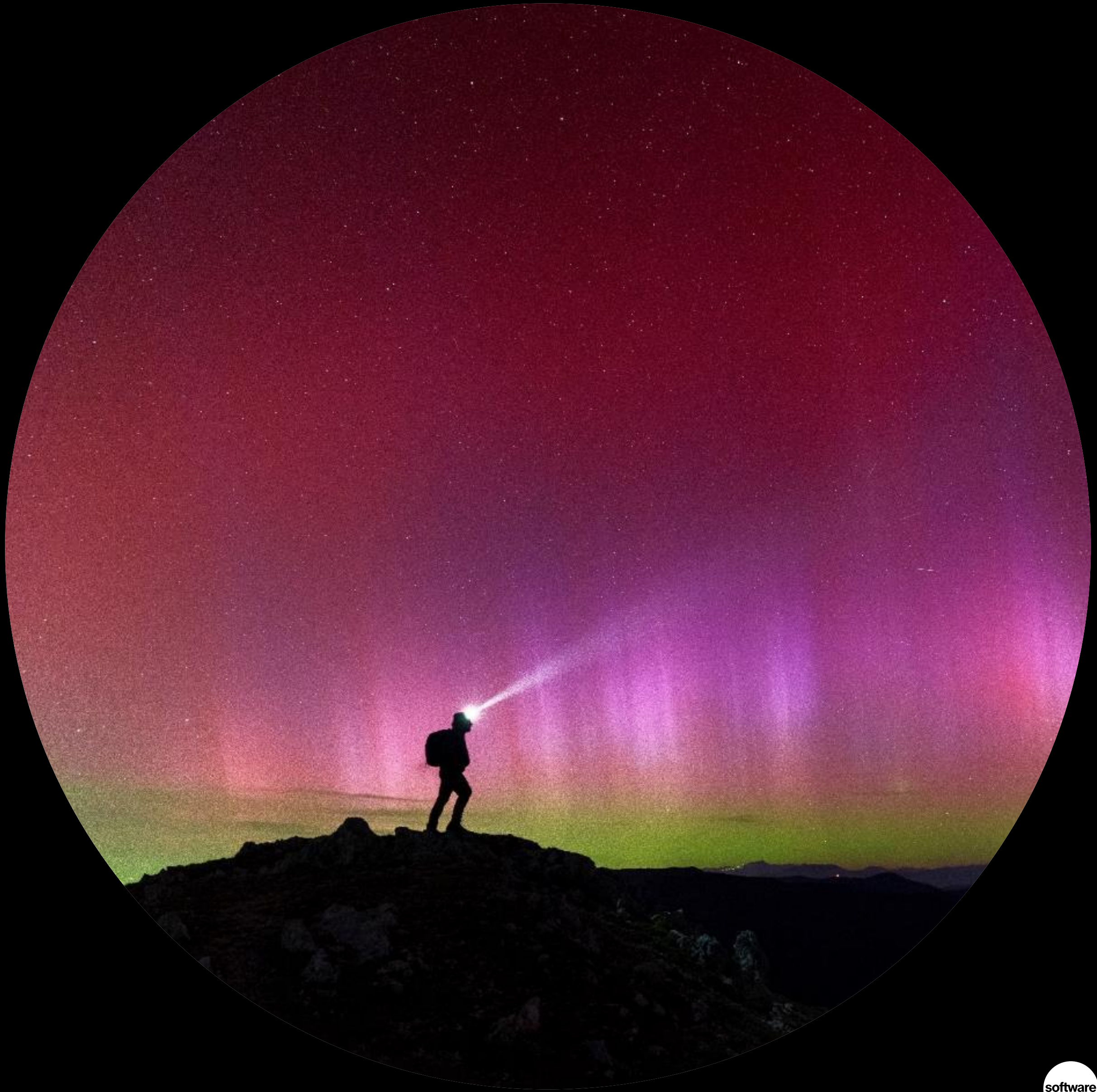
Linkdump:

Tools:
https://www.mailhardener.com/tools/
https://mxtoolbox.com
https://testconnectivity.microsoft.com/
https://internet.nl
https://dnssec-debugger.verisignlabs.com/
https://www.ssllabs.com/ssltest/
https://github.com/cammurray/orca

Guides:
Unused domain hardening guide
https://www.mailhardener.com/kb/hardening-unused-domains
EOP best practices
https://www.undocumented-features.com/2019/08/13/exchange-online-protection-eop-best-practices-and-recommendations

Pshell cmdlets:
https://www.azure365pro.com/adding-domains-in-bulk-to-microsoft-365-using-powershell/

MISC:
https://techcommunity.microsoft.com/blog/exchange/exchange-online-to-retire-basic-auth-for-client-submission-smtp-auth/4114750
https://techcommunity.microsoft.com/blog/exchange/upgrading-your-organization-from-current-versions-to-exchange-server-se/4241305
https://techcommunity.microsoft.com/blog/exchange/throttling-and-blocking-email-from-persistently-vulnerable-exchange-servers-to-e/3815328
https://bhr.62e.myftpupload.com/2018/12/19/checking-for-compromised-email-accounts/



Get in touch

+31 (0)20 25 86 800

Info_nl@softwareone.com

Naritaweg 177
1043 BW Amsterdam
The Netherlands

Disclaimer

This publication contains proprietary information that is protected by copyright. SoftwareOne reserves all rights thereto.

SoftwareOne shall not be liable for possible errors in this document. Liability for damages directly and indirectly associated with the supply or use of this document is excluded as far as legally permissible.

The information presented herein is intended exclusively as a guide offered by SoftwareOne. The publisher's product use rights, agreement terms and conditions and other definitions prevail over the information provided herein. The content must not be copied, reproduced, passed to third parties or used for any other purposes without written permission of SoftwareOne