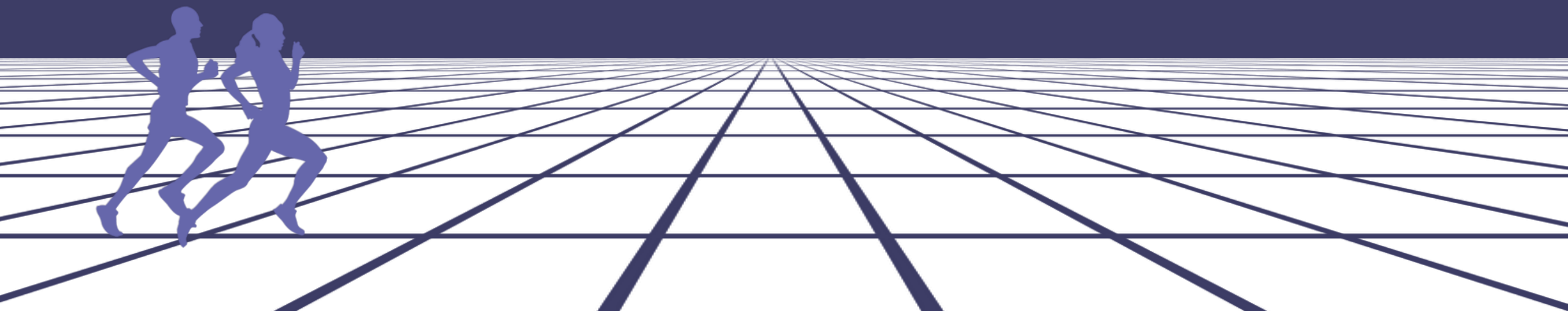
MICROSOFT 365 VIRTUAL MARATHON 2022

MAY, 4 – 6, 2022

Peter Schmidt
NeoConsulting

Protecting Your Users Against Phishing Attacks



MICROSOFT 365 VIRTUAL MARATHON 2022 SPONSORS

AvePoint

KnowledgeLake

VisualSP™

TEAMS HUB
– by cyclotron –

EMPEROR MEDIA GROUP

PowerUP! Learning
Why Just Train? emPower!

LION TECH
Business Transformation Leaders

SMARTER CONSULTING

iTProve
Improving knowledge for you.

Peter Schmidt

MVP MCM MCSM MCT

Cloud Architect @NeoConsulting, Denmark

- Cloud Architect
- MVP: Office Apps & Services
- MCM: Exchange, MCSM: Exchange, MCT
- Blog: www.msdigest.net
- Twitter: @petsch

Agenda

- Intro
- Spoofing & Phishing
- SPF / DKIM / DMARC
- Defender for Office 365
- DEMO
- Summary

What Are We Talking About?

Phish	• The fraudulent attempt to obtain sensitive information
Spoofing	• Creation of email messages with a forged sender address
Impersonation	• Common technique in targeted phishing attacks
Authentication	• A way to prove the sender really is the sender
SPF	• Sender Policy Framework
DKIM	• DomainKeys Identified Mail
DMARC	• Domain Message Authentication Reporting & Conformance

Types of Phishing

CLONE PHISHING

CLONE PHISHING IS WHERE A LEGITIMATE, AND PREVIOUSLY DELIVERED, BIT OF ONLINE CORRESPONDENCE IS USED TO CREATE AN ALMOST IDENTICAL OR "CLONE" EMAIL.

SPEAR PHISHING

SPEAR PHISHING IS A PHISHING ATTEMPT DIRECTED AT A PARTICULAR INDIVIDUAL OR COMPANY.

WHALING

WHALING IS A PHISHING ATTEMPT DIRECTED SPECIFICALLY AT A SENIOR EXECUTIVE OR ANOTHER HIGH-PROFILE TARGET WITHIN A BUSINESS.

Phishing Insights

- Most common disguises:
  - Bill / invoice (15.9%)
  - Email delivery failure (15.3%)
  - Legal / law enforcement (13.2%)
  - Scanned document (11.5%)
  - Package delivery (3.9%)

- The most common malicious attachment types:
  - Office
  - Archive
  - PDF

What is the issue ?

SMTP has always, by default, been anonymous

You can easily send an email pretending it came from someone else

“Proper” use of this include outsourced marketing and mailing lists

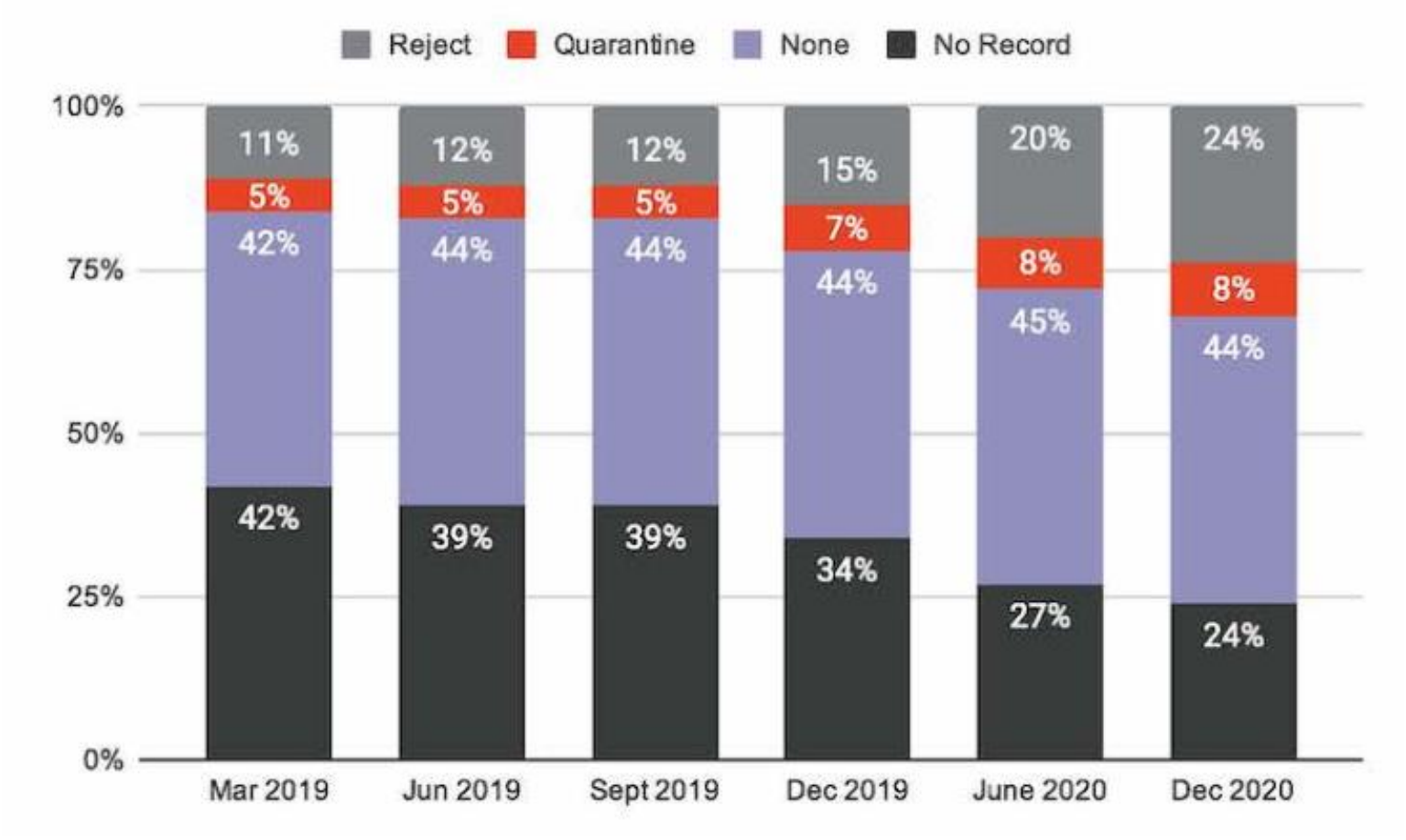
Its difficult to implement this well and the perceived complexity means that companies worry their email will get blocked if they implement it badly

How Do We Authenticate Emails We Receive

SPF	• v=spf1 ip4:1.2.5.5 ip4:8.2.7.4 ip4:7.3.2.2 ip4:5.5.1.8 include:_spf.salesforce.com include:spf.protection.outlook.com -all
DKIM	• "v=DKIM1; p=MIGfMA0GDQEBgQCrZ6z … 6UvqP3QIDAQAB"
DMARC	• v=DMARC1; p=reject; rua=mailto:dmarc@dmarc-aggregator.com; ruf=mailto:dmarc-ruf@dmarc-aggregator.com

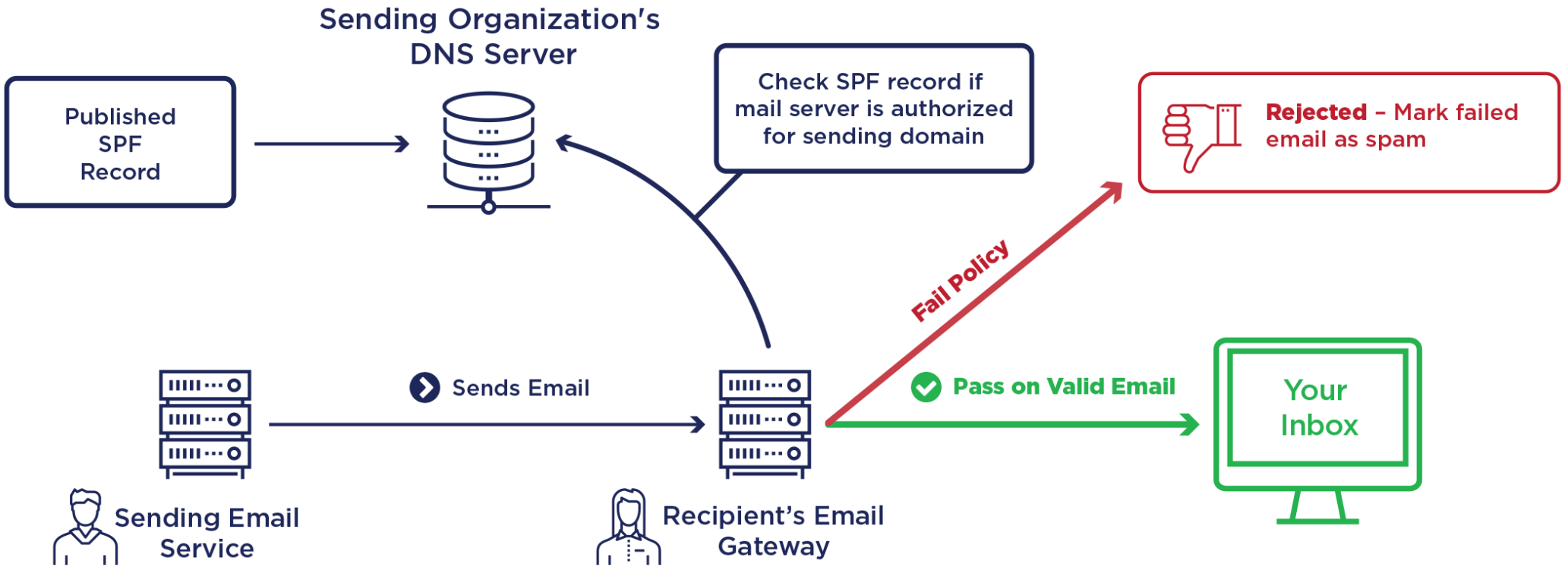
To send email to Microsoft (i.e. to an Office 365 user or Outlook.com) then you need to implement this to stop your email being marked as spam

DMARC Policies of Fortune 500 Companies

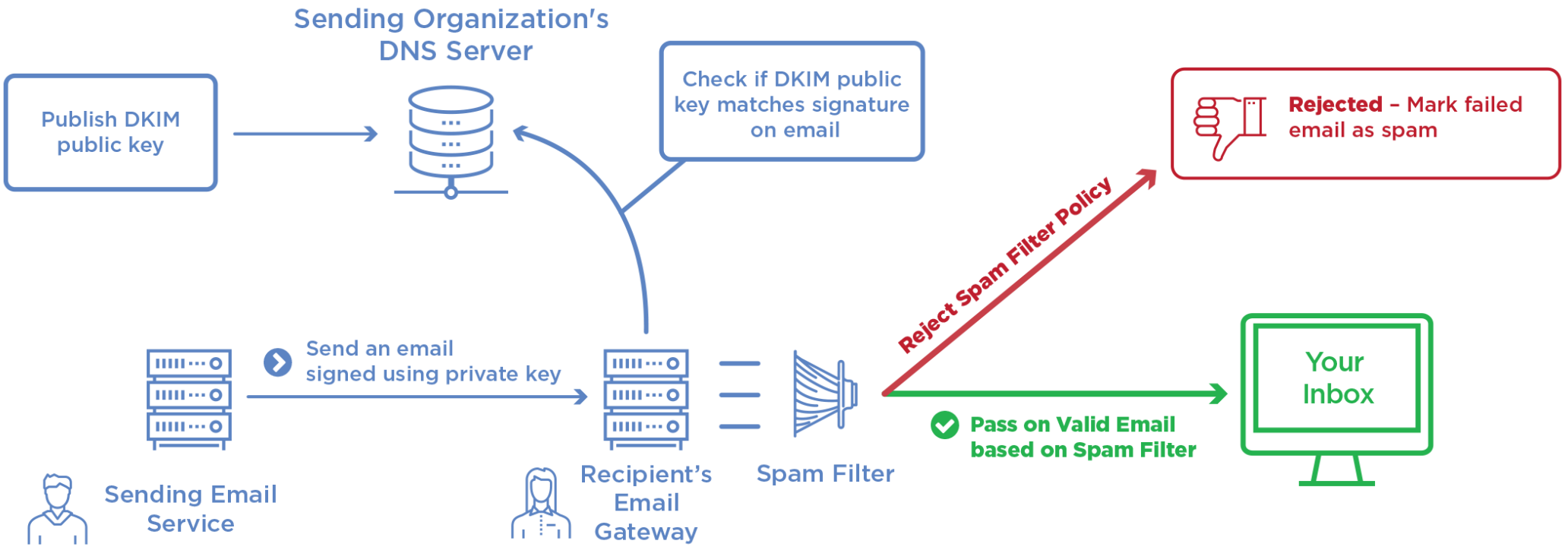


Numbers from Agari May 2021

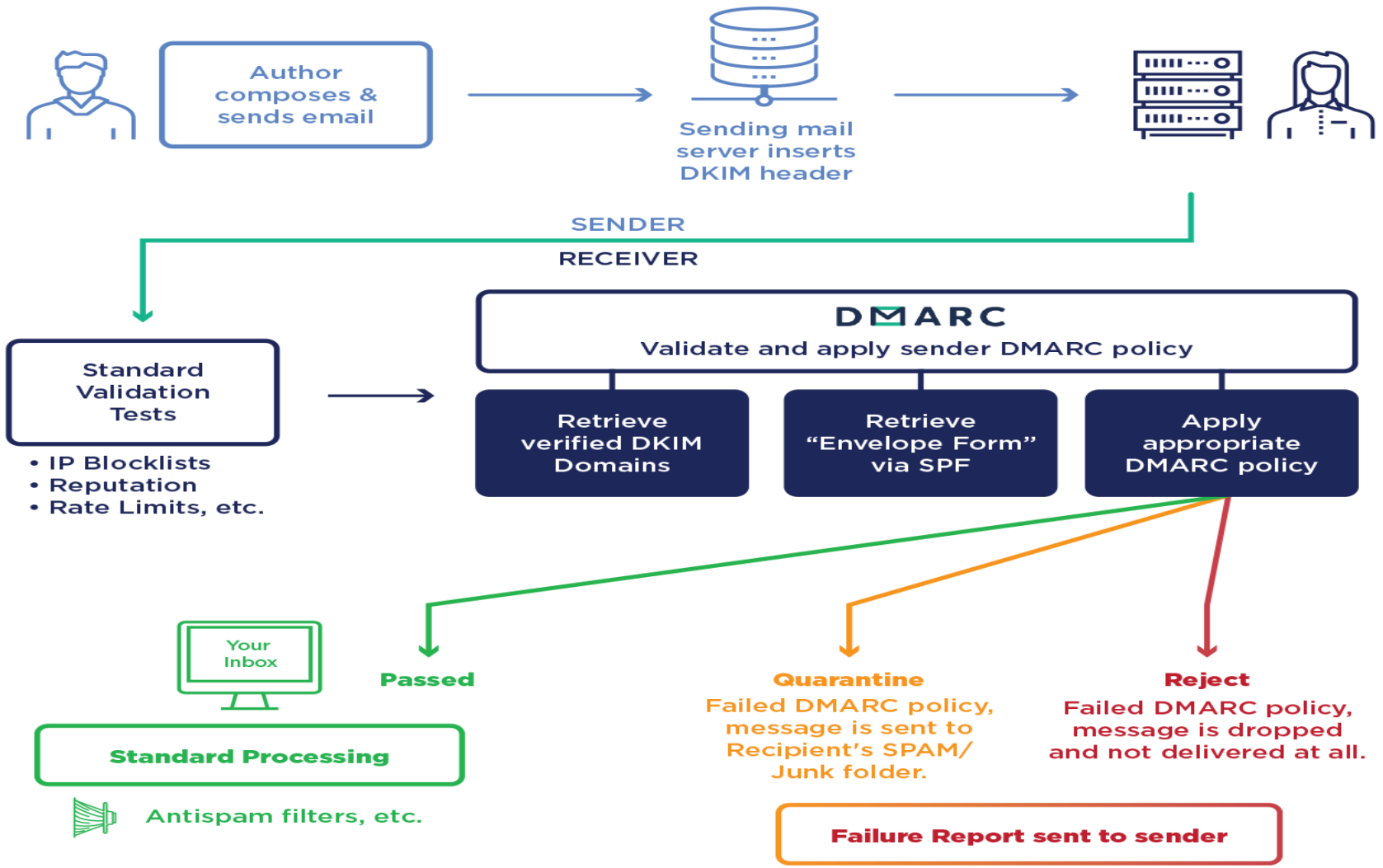
Sender Policy Framework (SPF)



DKIM


Sending Organization's DNS Server
Publish DKIM public key
Check if DKIM public key matches signature on email
Rejected – Mark failed email as spam
Reject Spam Filter Policy
Send an email signed using private key
Your Inbox
Pass on Valid Email based on Spam Filter
Sending Email Service
Recipient's Email Gateway
Spam Filter

DMARC


Author composes & sends email
Sending mail server inserts DKIM header
SENDER
RECEIVER
Standard Validation Tests
• IP Blocklists
• Reputation
• Rate Limits, etc.
DMARC
Validate and apply sender DMARC policy
Retrieve verified DKIM Domains
Retrieve "Envelope Form" via SPF
Apply appropriate DMARC policy
Your Inbox
Passed
Standard Processing
Antispam filters, etc.
Quarantine
Failed DMARC policy, message is sent to Recipient's SPAM/ Junk folder.
Reject
Failed DMARC policy, message is dropped and not delivered at all.
Failure Report sent to sender

Microsoft Defender for Office 365 (MDO)

Exchange Online Protection

Preventing broad and volume-based & known attacks

MDO P1

Protects email and collaboration from zero-day malware, phish, and business email compromise

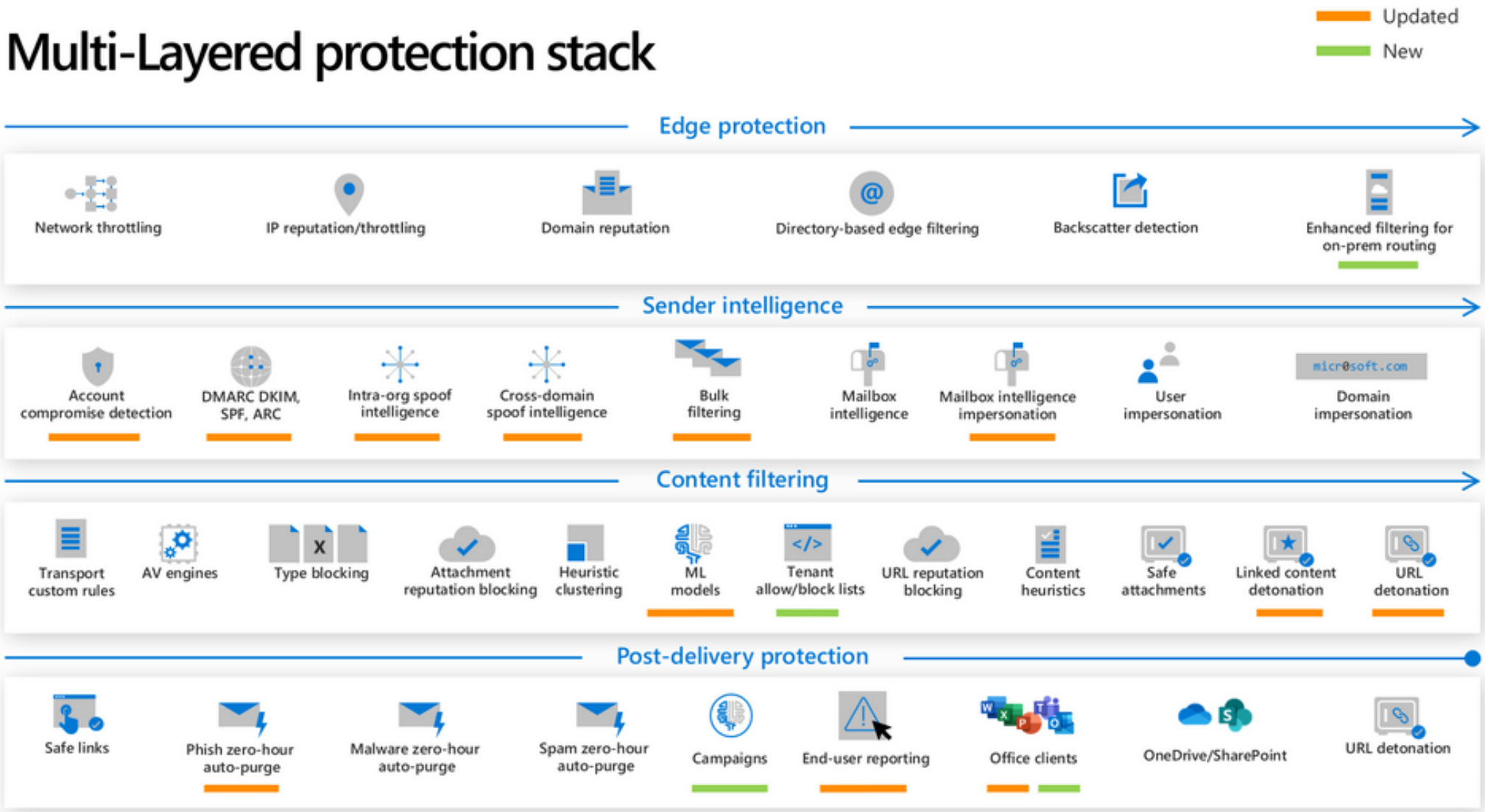
MDO P2

Adds post-breach investigation, hunting, and response, as well as automation, and simulation (for training)

Microsoft Defender for Office 365

- Microsoft is positioned as a leader in The Forrester Wave™: Enterprise Email Security, Q2 2021
- Microsoft Defender for Office 365 received the highest possible score in the incident response, threat intelligence, and endpoint and endpoint detection and response (EDR) solutions integration criteria, as well as in the product strategy, customer success, and performance and operations criteria.

Defender for Office 365 Protection Stack



Anti-Spoofing in Exchange Online

Exchange Online Protection (EOP) Anti-Spoofing Capabilities

Defender for Office 365

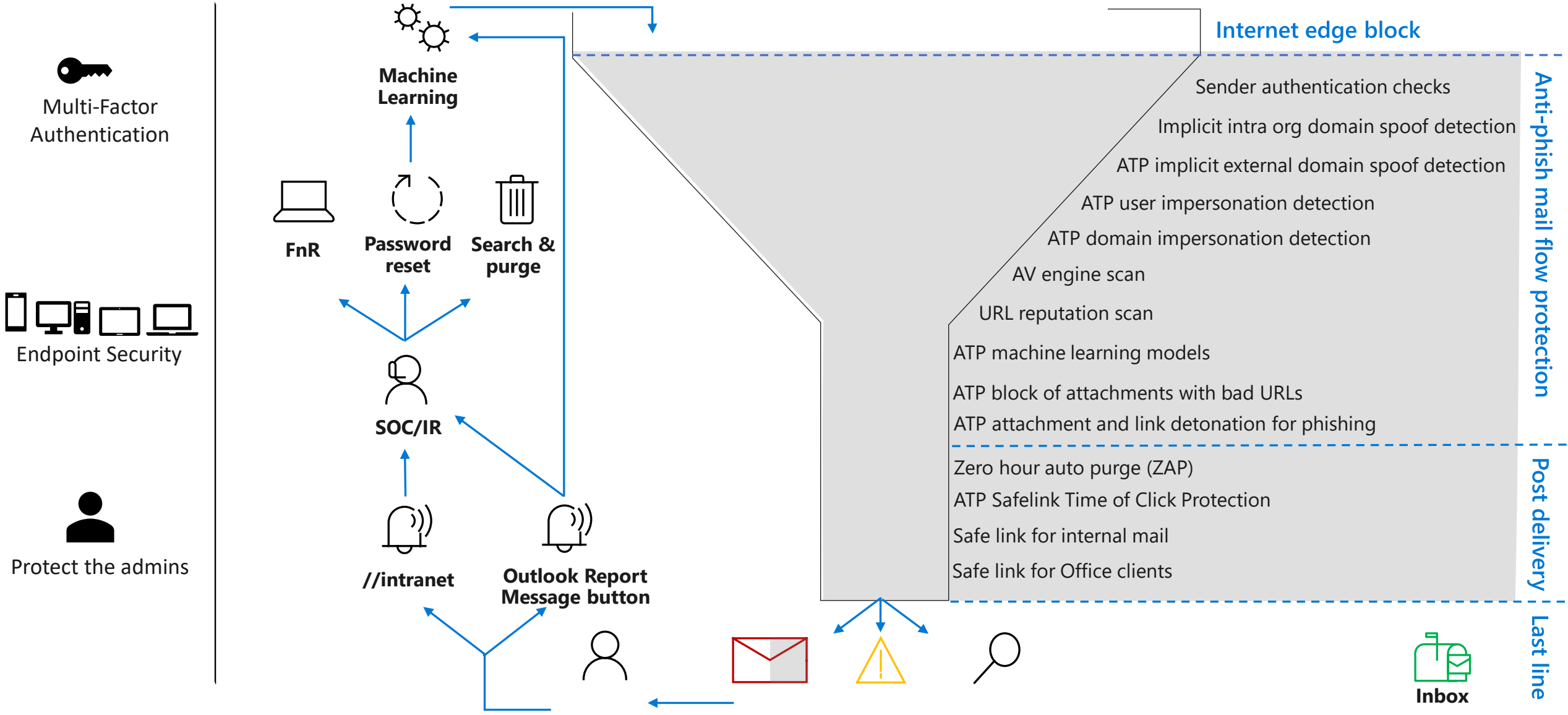
Composite Authentication (compauth) – aka Machine Learning

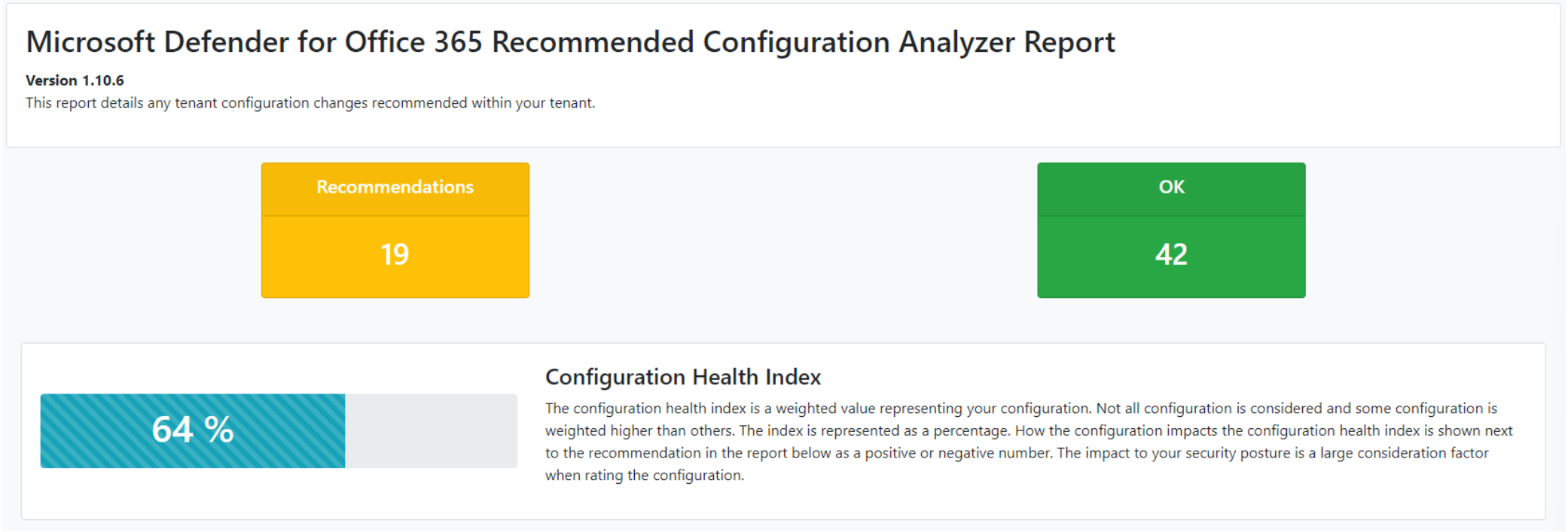
- MDO and EOP Anti-Spoof Protection. Microsoft using the power of the cloud to determine if spoofed email
- Default Anti-Phish Policy
- Additional Policies

How To Configure

- In the Office 365 Security
- Via PowerShell

Phishing protection end-to-end



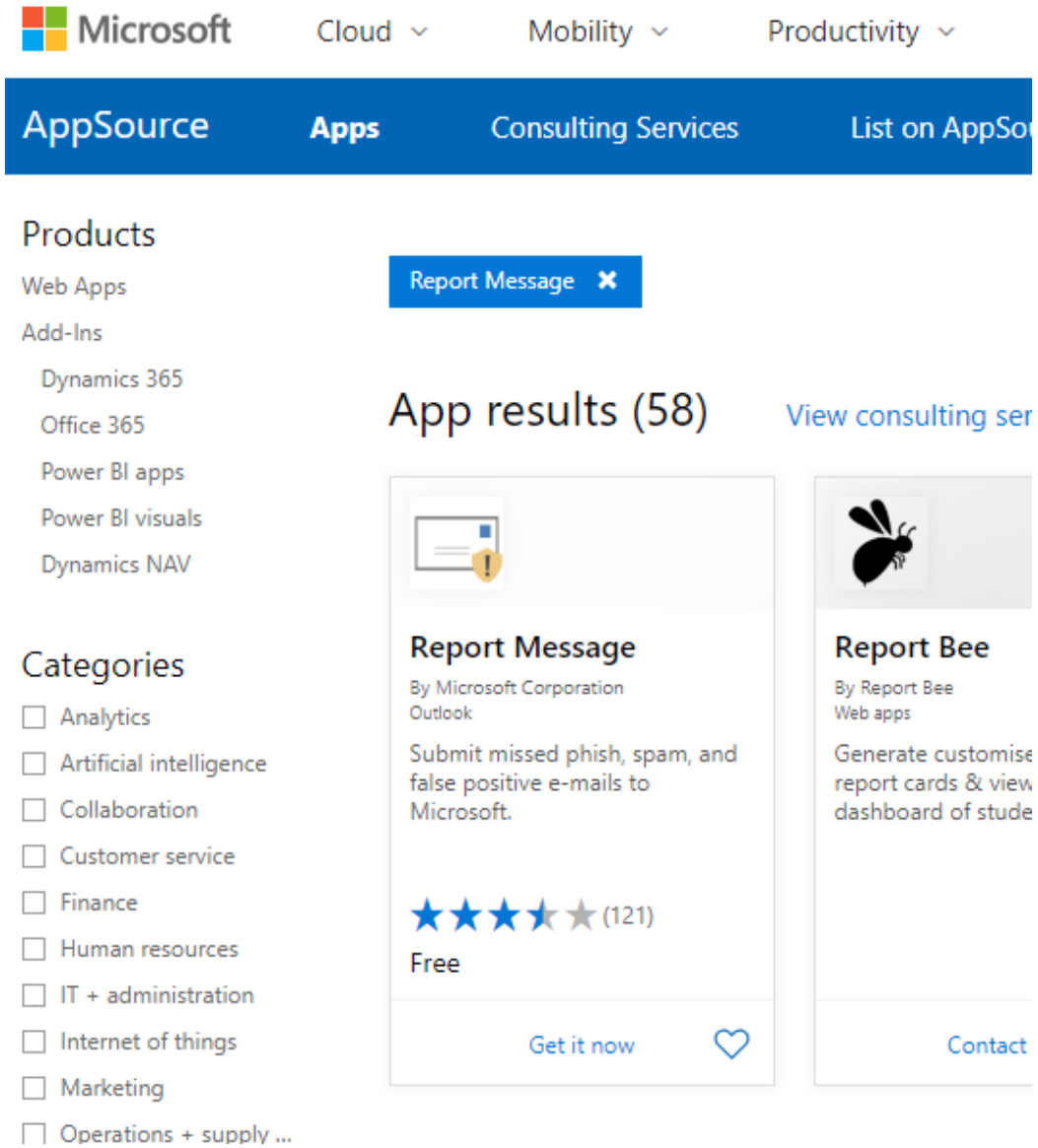


Configuration Analyzer

- Threat Policies – Configuration Analyzer
- Office 365 Advanced Threat Protection Recommended Configuration Analyzer (ORCA)
- Install in PowerShell using:
  - Install-Module -Name ORCA

This all sounds hard - how to get started

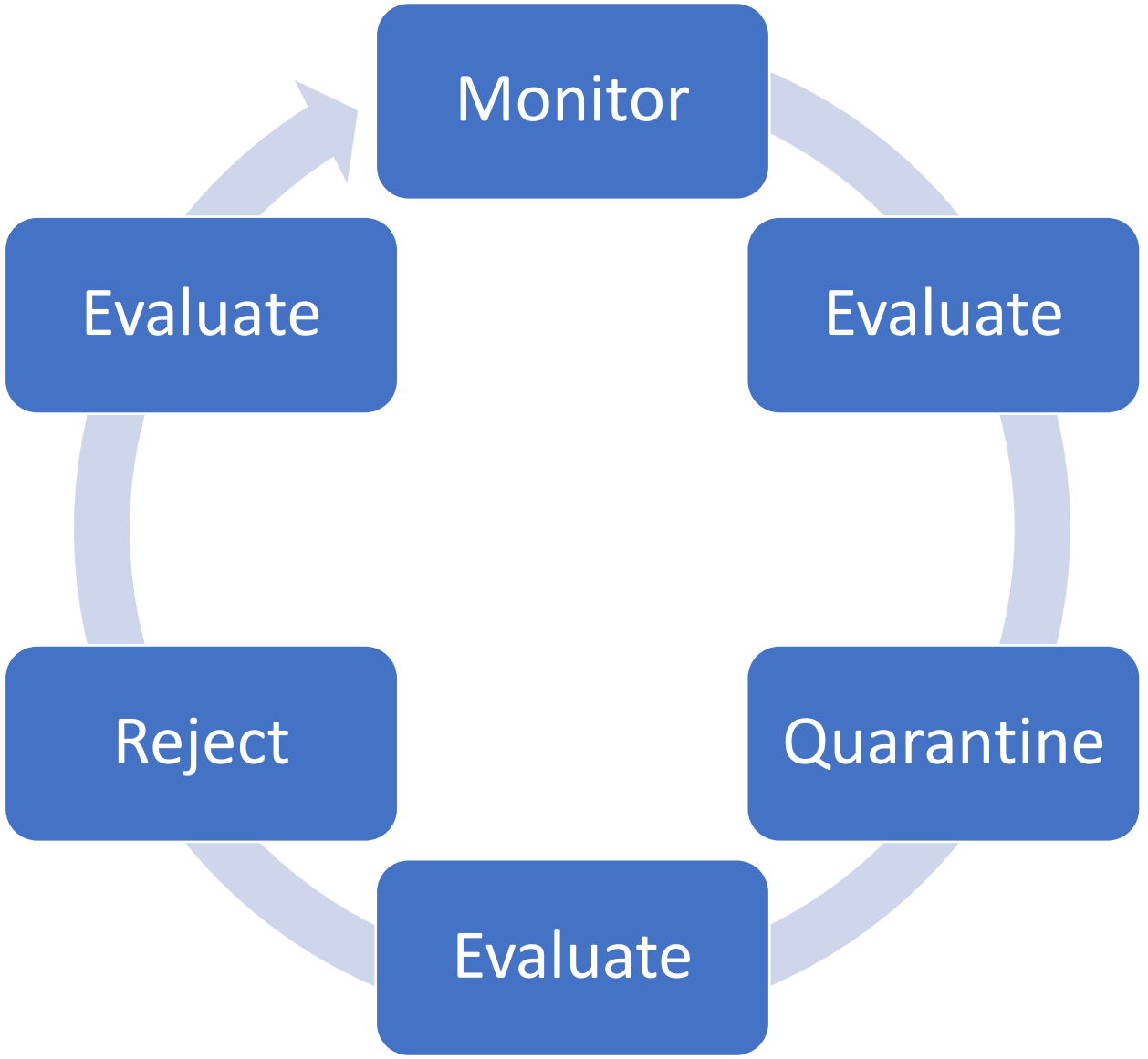
- SPF, DKIM
- DMARC
- Office 365
  - Anti-Spoof
  - Anti-Phishing
  - Report Add-in
  - Configuration Analyzer



- Let’s have a look at:
  - SPF
  - DKIM
  - DMARC

- MDO Impersonation
- MDO Configuration

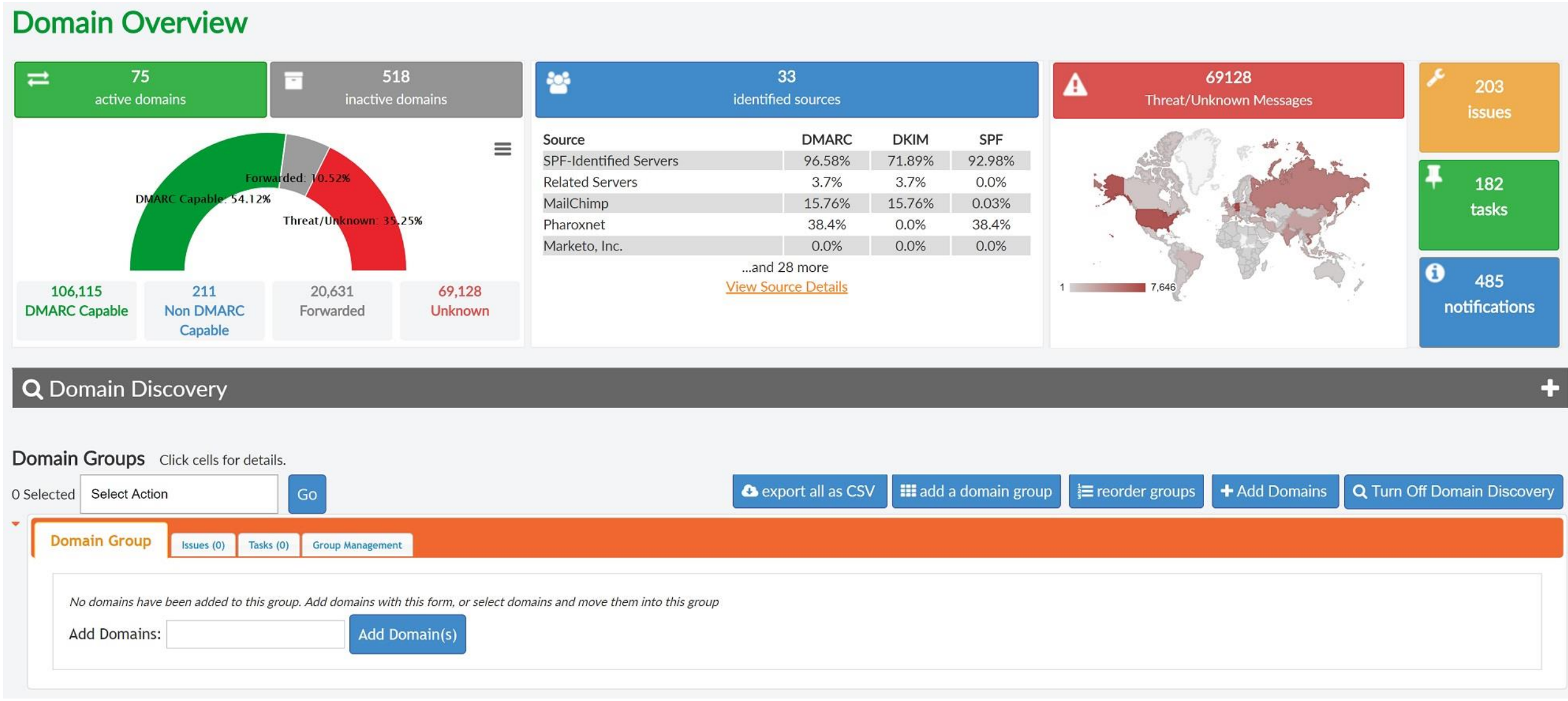
Implementing DMARC in phases



DMARC Analyzers

- Reporting and Analyzer tool for overview
- Some of the tools available:
  - DmarcAnalyzer
    - www.dmarcanalyzer.com
  - PostMarkApp
    - https://dmarc.postmarkapp.com
  - EasyDmarc
    - https://easydmarc.com/
  - MXToolbox
    - https://mxtoolbox.com/dmarcsetup
  - Dmarcian
    - www.dmarcian.com
  - ValiMail
    - https://www.valimail.com/office-365-free-dmarc-monitoring/

DMARC Report Example



User Awareness

Simulations

- ✓ Construct mails that match the level of sophistication that is trending in the wild.
- ✓ Data is your best friend. Use exercise results to determine your next move.
- ✓ Might as well test “the system” while you’re at it!

Training

- ✓ Leverage large scale training programs for in-depth education.
- ✓ Phishing isn’t just an email thing - include guidance on attack vectors such as “Smishing” and “Vishing”.
- ✓ Keep the conversation going through ongoing awareness campaigns.

Reporting

- ✓ What’s your 911? Make sure your community knows when and how to report.
- ✓ Make reporting as quick and easy as possible.
- ✓ Use reporting trends to inform program needs.

Best Practices

- Architectural design of your mail flow and domains
- Use both SPF and DKIM
- Use DMARC authorization record
- Do this for all your domains

- Common mistakes:
  - DMARC needs SPF and DKIM to succeed
- Follow-up on DMARC Reports and Reports in Office 365

- Microsoft Office Defender for 365
  - Phishing
  - ORCA reports

SPF
Best Practice

- Simple SPF: v=spf1 include:spf.protection.outlook.com -all

- More Advanced SPF:
  - **neoconsulting.dk**: v=sf1 include:spf-internal.neoconsulting.dk include:spf-external.neoconsulting.dk -all
  - **spf-internal.neoconsulting.dk**: v=spf1 include:spf.protection.outlook.com ip4:37.123.123.4 ip4:37.123.123.5 -all
  - **spf-external.neoconsulting.dk**: v=spf1 include:sendgrid.net a:c.spf.service-now.com -all

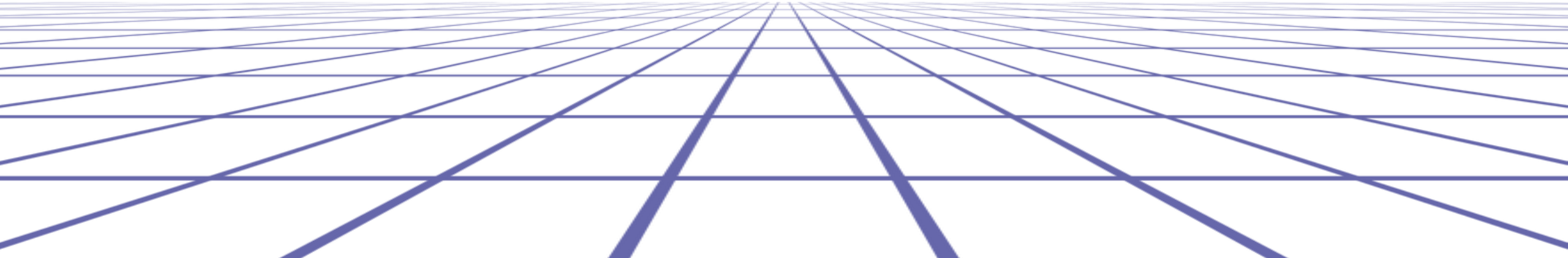
How Can We Protect Our Users ?

- MDO features
  - MDO for Safe Links and Safe Attachments
  - Anti-Phishing Features
  - Attack Simulator and training
- Multi-Factor Authentication
- Conditional Access
- Stopping Weak Password, Legacy Auth etc.
- Authenticators and Hardware Tokens
- E-mail Encryption (TLS) and Office 365 Message Encryption

Lessons Learned

- SPF, DKIM, DMARC is important
- Plan your DMARC
- Defender for Office 365
- User Awareness Campaigns
- Report Spam – End User
- Phishing Campaigns / Attack Simulations

QUESTIONS



Feedback

https://forms.office.com/r/zzULt1dHLi