



May 31 – June 2, Oslo Spektrum
10th anniversary

Peter Schmidt & Michael Mardahl

Deep Dive into Defender for Office & Authenticated E-mail

About Peter



Peter Schmidt
Cloud Architect
NeoConsulting



Microsoft MVP: Office Apps & Services
MCM & MCSM: Exchange
Microsoft Certified Trainer (MCT)

Contact Me

Twitter: @petsch

Blog: <https://www.msdigest.net/>

Mail: peter@neoconsulting.dk

About Michael

Michael Mardahl
Cloud Architect
APENTO



Microsoft MVP: Enterprise Mobility (Identity)
Microsoft Certified Trainer (MCT)
Certified ISO 27001 Lead Implementer

Contact Me

Twitter: @michael_mardahl

Blog: <https://www.msendpointmgr.com/>

Mail: mum@apento.com

Agenda

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

Let's agree on some terminology and technology!

Phish	• The fraudulent attempt to obtain sensitive information
Spoofing	• Creation of email messages with a forged sender address
Impersonation	• Common fraud 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
BIMI	• Brand Indicators for Message Identification
DNSSEC	• DNS Security Extensions

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



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

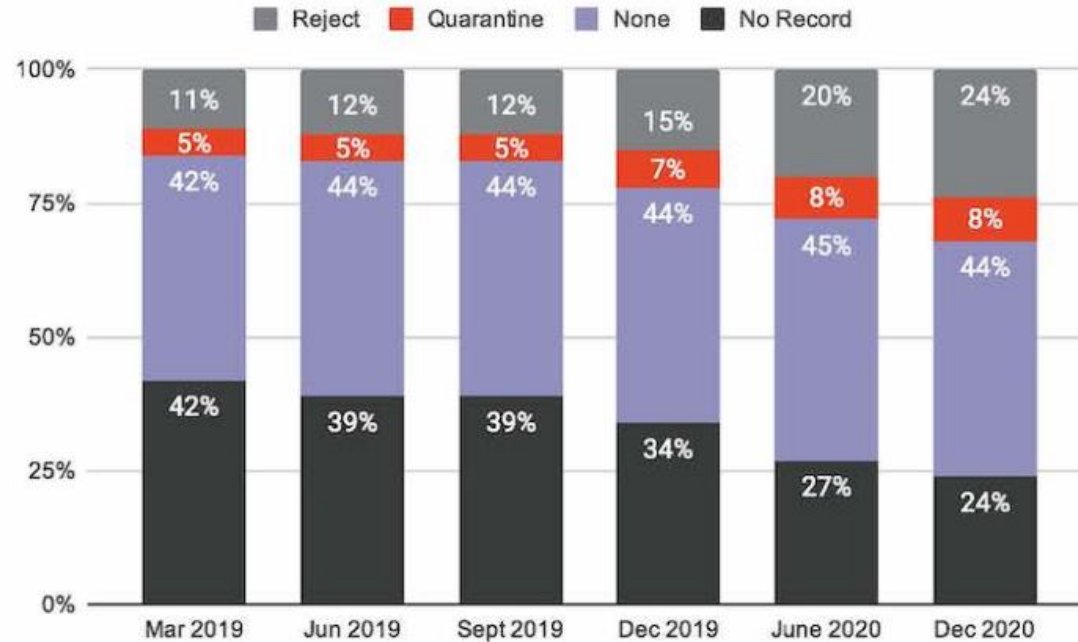
- `"v=DKIM1; p=MIGfMA0GDQEBgQCrZ6z ... 6UvqP3QIDAQAB"`

DMARC

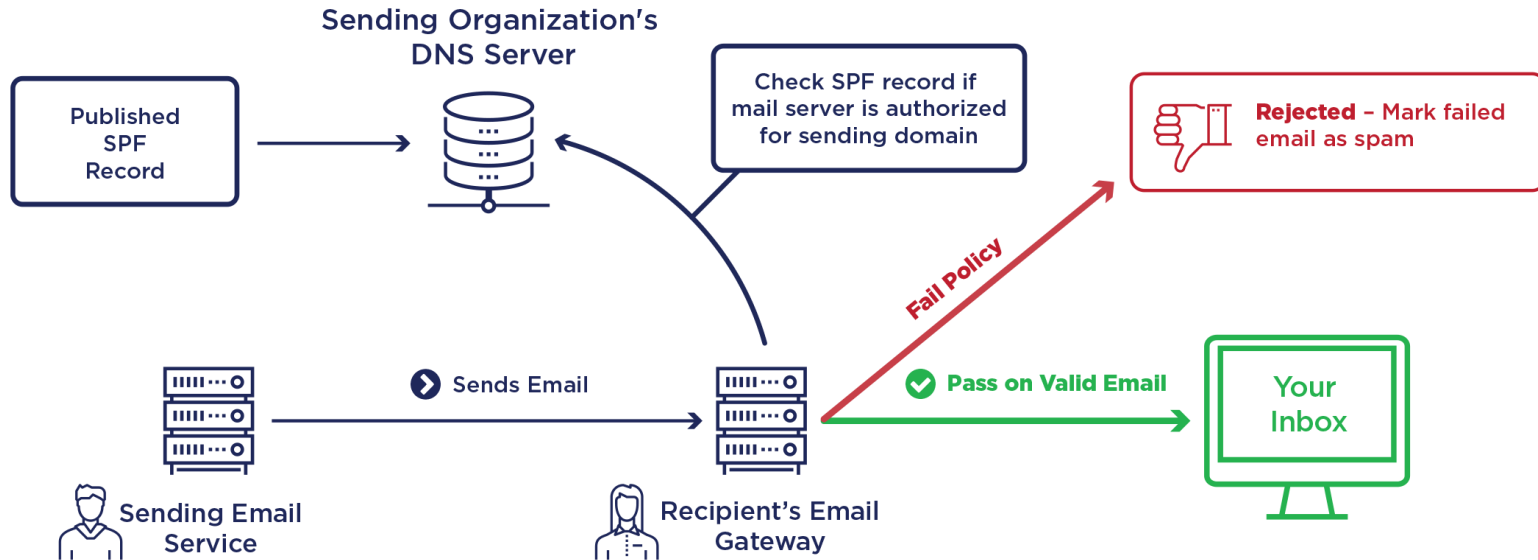
- `v=DMARC1; p=reject; rua=mailto:dmarc@dmarc-aggregator.com; ruf=mailto:dmarc-ruf@dmarc-aggregator.com`

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

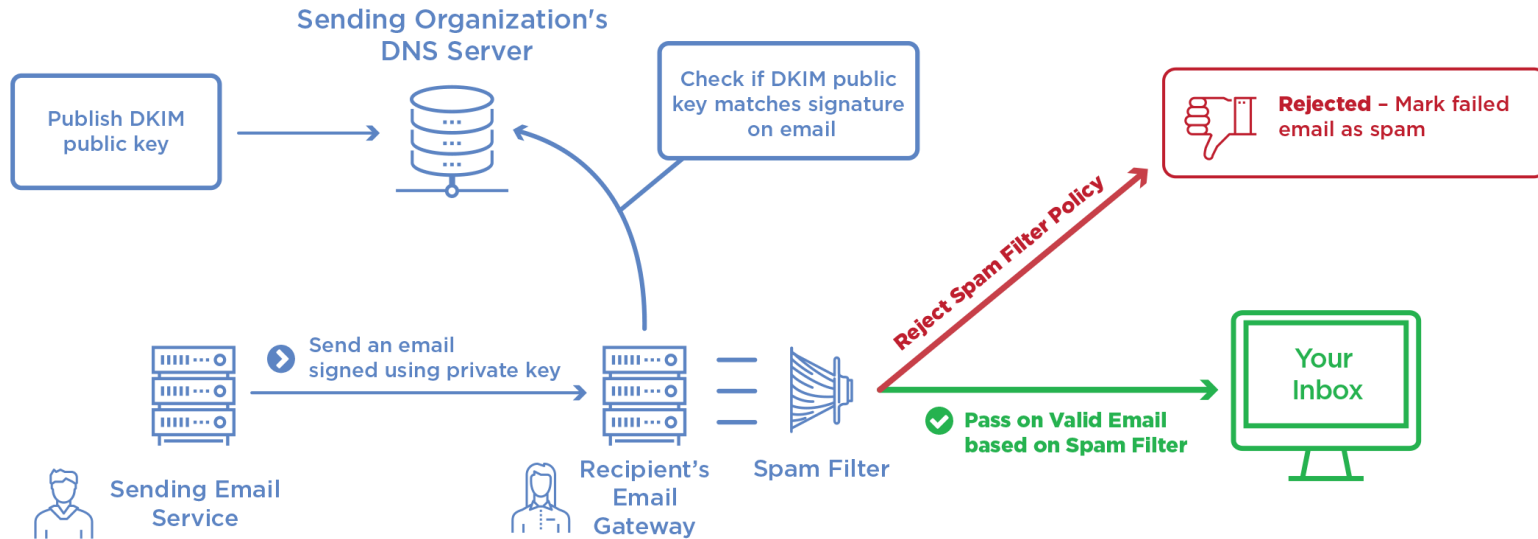
DMARC Policies of Fortune 500 Companies



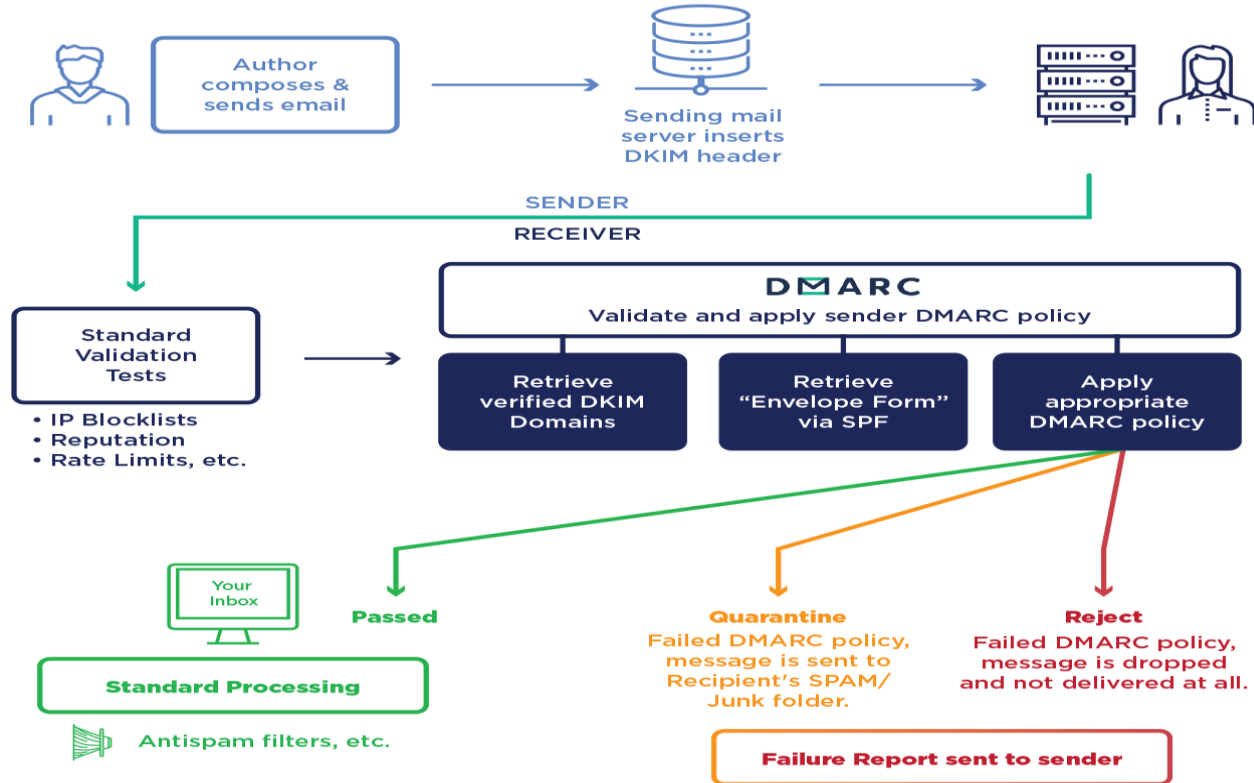
Sender Policy Framework (SPF)



DKIM



DMARC



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

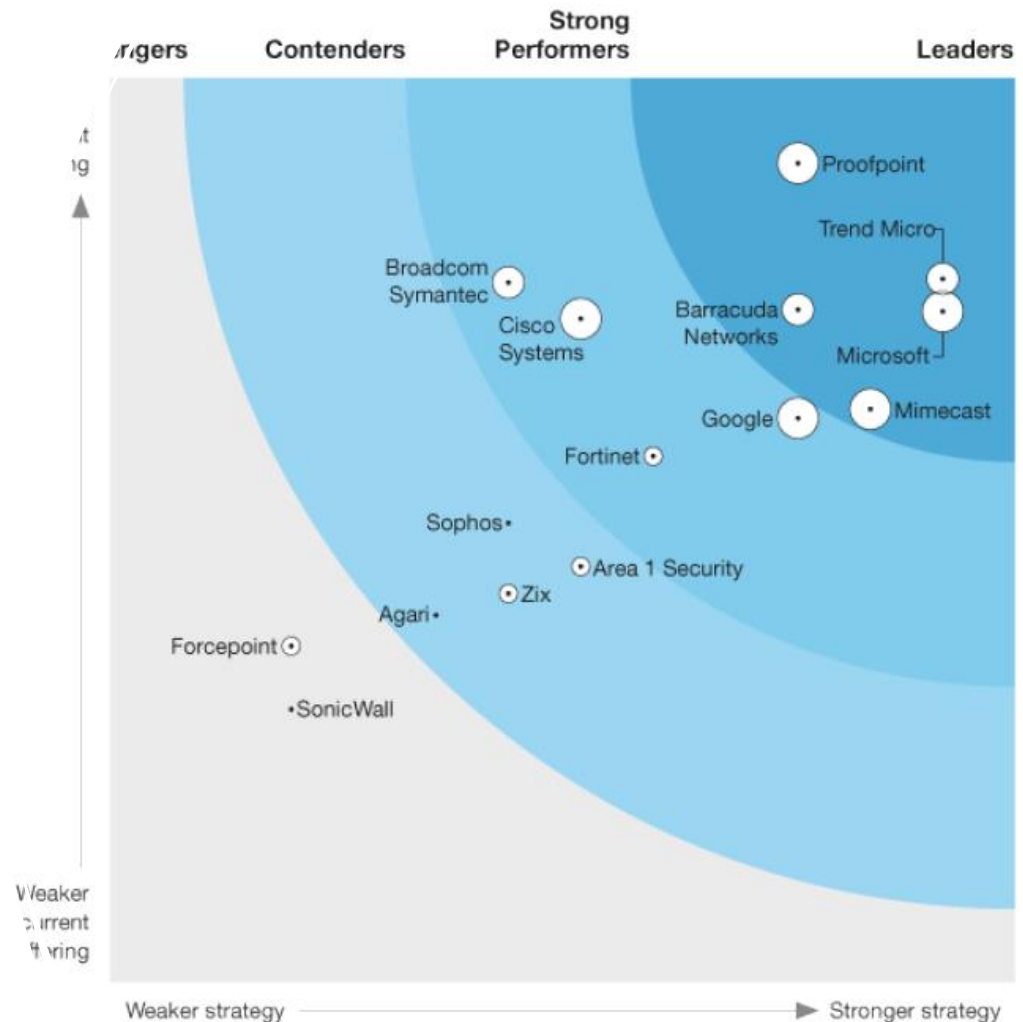


MDO P2

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.

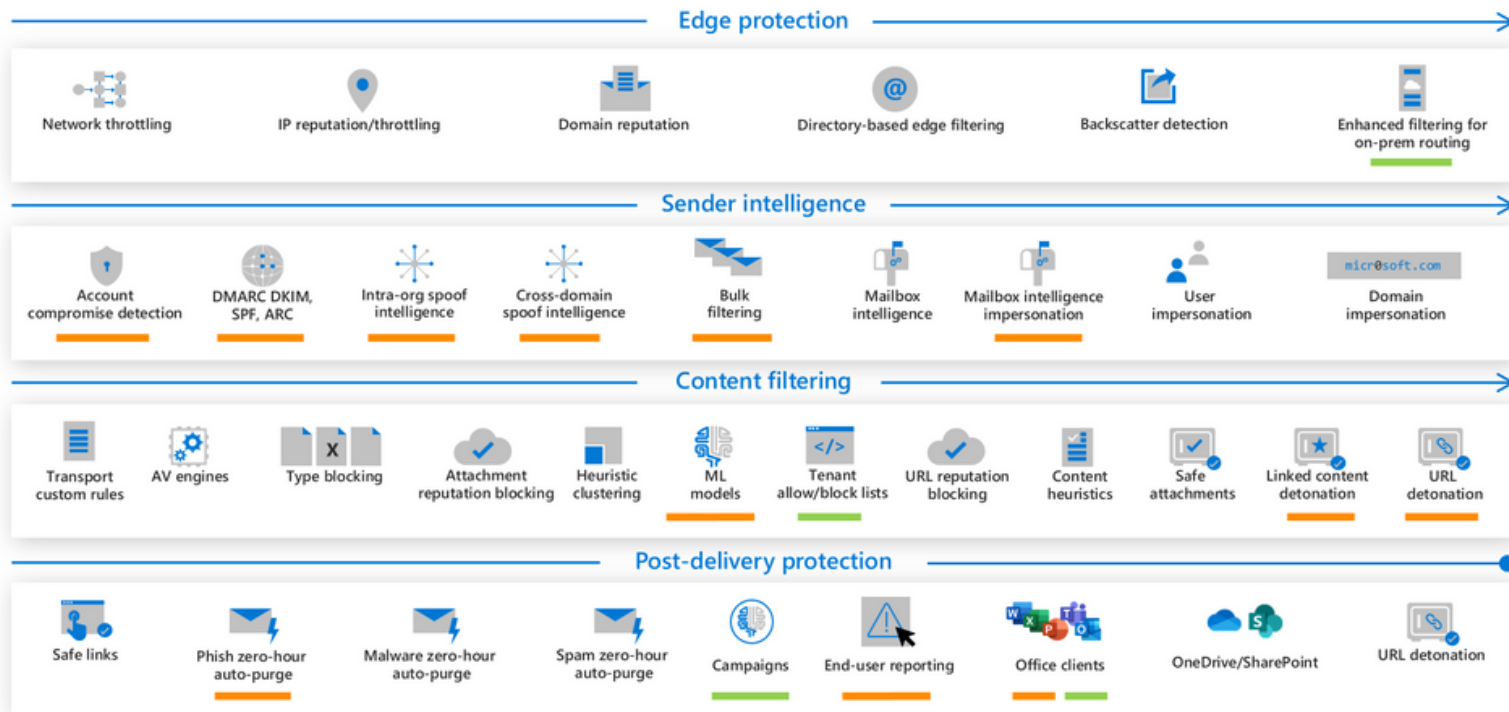


Defender for Office 365 Protection Stack

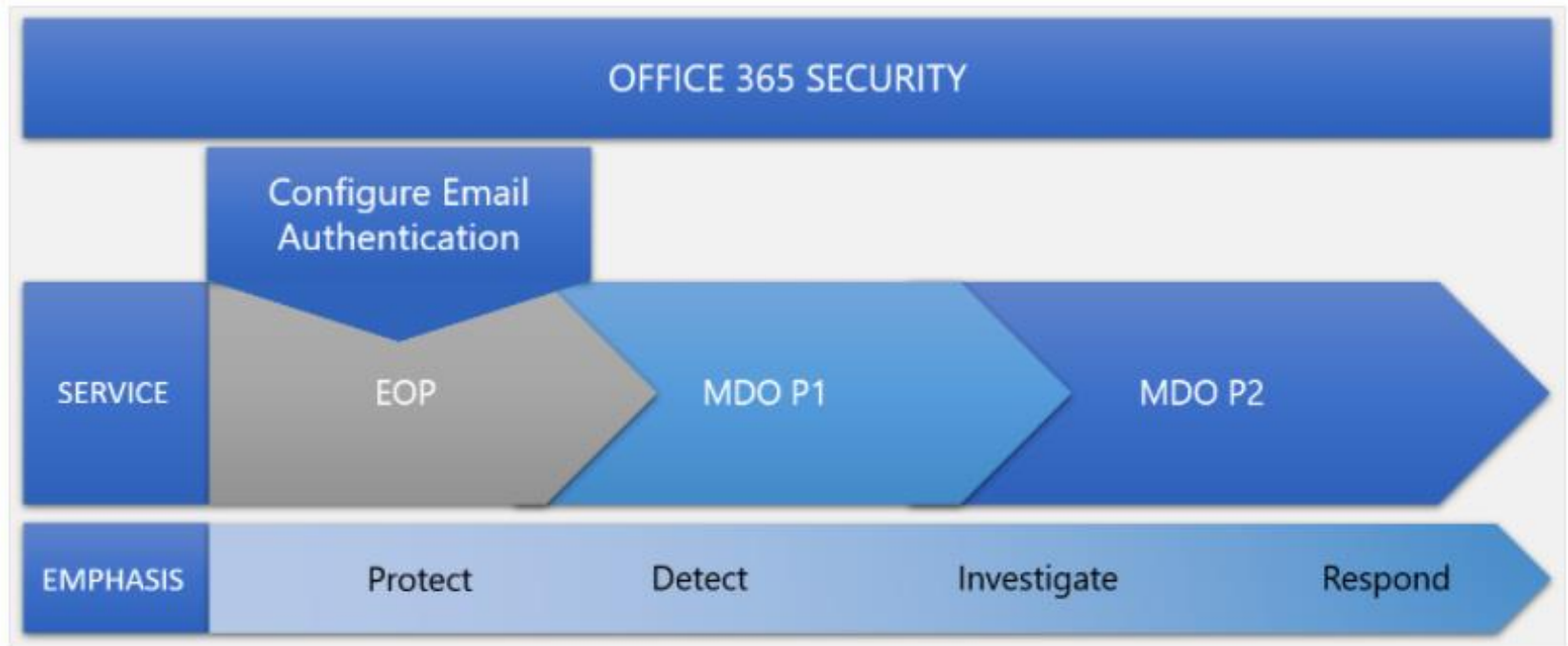
Multi-Layered protection stack

Updated

New



E-mail Security in Office 365



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

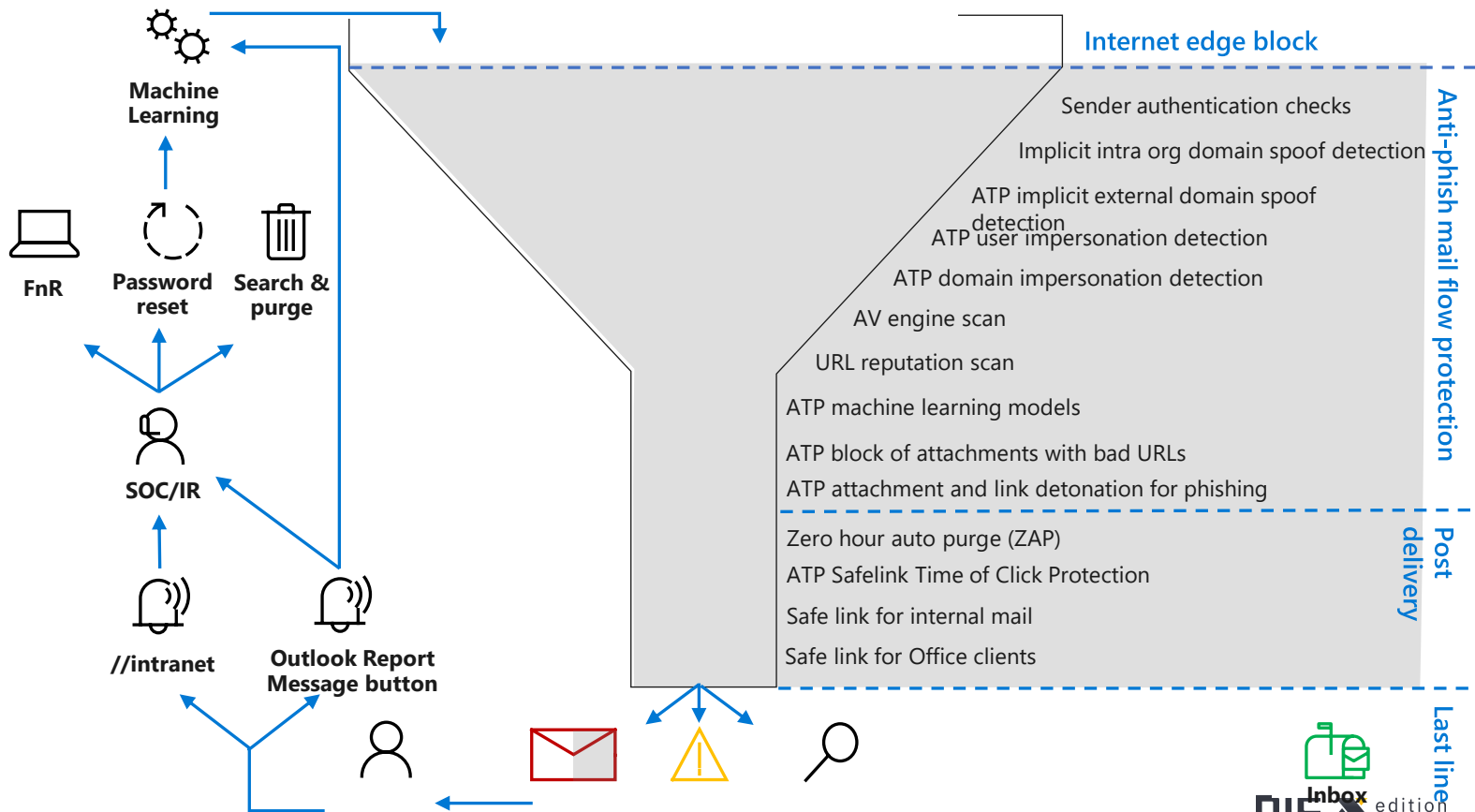
- In the Office 365 Security
- Via PowerShell

Phishing protection end-to-end


Multi-Factor
Authentication


Endpoint Security


Protect the admins



Microsoft Defender for Office 365 Recommended Configuration Analyzer Report

Version 1.10.6

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

Recommendations

19

OK

42

64 %

Configuration Health Index

The configuration health index is a weighted value representing your configuration. Not all configuration is considered and some configuration is weighted higher than others. The index is represented as a percentage. How the configuration impacts the configuration health index is shown next to the recommendation in the report below as a positive or negative number. The impact to your security posture is a large consideration factor when rating the configuration.

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

The screenshot shows the Microsoft AppSource interface. At the top, there's a navigation bar with the Microsoft logo and links for Cloud, Mobility, and Productivity. Below this is a blue header with 'AppSource', 'Apps', 'Consulting Services', and 'List on AppSource'. The main content area is divided into 'Products' and 'Categories'. Under 'Products', there are links for Web Apps, Add-Ins, Dynamics 365, Office 365, Power BI apps, Power BI visuals, and Dynamics NAV. Under 'Categories', there's a list of checkboxes for various business functions like Analytics, Artificial intelligence, Collaboration, Customer service, Finance, Human resources, IT + administration, Internet of things, Marketing, and Operations + supply ... The 'App results (58)' section shows two app cards. The first card is for 'Report Message' by Microsoft Corporation Outlook, with a 4.5-star rating (121 reviews) and a 'Free' price tag. It has a 'Get it now' button and a heart icon. The second card is for 'Report Bee' by Report Bee Web apps, with a 'Contact' button. A 'Report Message' button is also visible in the top right of the app results section.

Microsoft Cloud Mobility Productivity

AppSource Apps Consulting Services List on AppSource

Products

Web Apps

Add-Ins

Dynamics 365

Office 365

Power BI apps

Power BI visuals

Dynamics NAV

Categories

- ☐ Analytics
- ☐ Artificial intelligence
- ☐ Collaboration
- ☐ Customer service
- ☐ Finance
- ☐ Human resources
- ☐ IT + administration
- ☐ Internet of things
- ☐ Marketing
- ☐ Operations + supply ...

App results (58) View consulting ser

Report Message

By Microsoft Corporation Outlook

Submit missed phishing, spam, and false positive e-mails to Microsoft.

★★★★★ (121)

Free

Get it now

Report Bee

By Report Bee Web apps

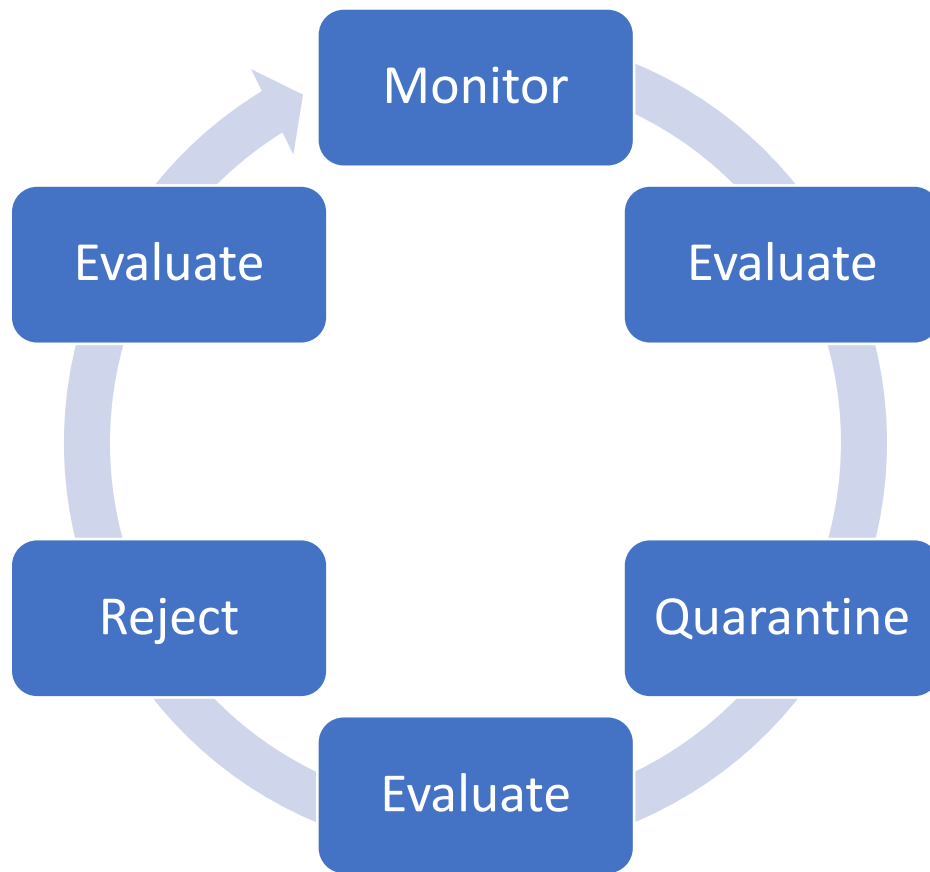
Generate customise report cards & view dashboard of stude

Contact

- Let's have a look at:
 - SPF
 - DKIM
 - DMARC
- MDO Impersonation
- MDO Configuration
- Attack Simulations

DEMO

Implementing DMARC in phases

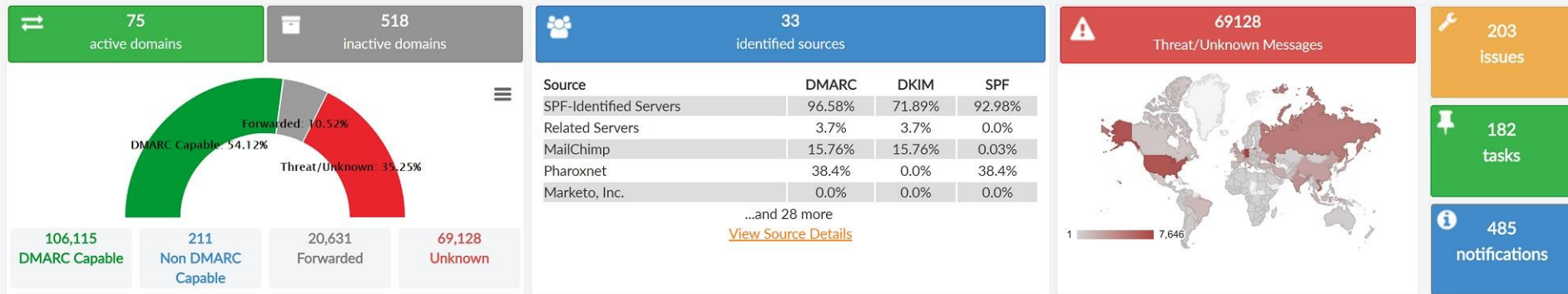


DMARC Analyzers

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

DMARC Report Example

Domain Overview



Domain Discovery

Domain Groups Click cells for details.

0 Selected

Select Action

Go

export all as CSV

add a domain group

reorder groups

+ Add Domains

Turn Off Domain Discovery

Domain Group

Issues (0)

Tasks (0)

Group Management

No domains have been added to this group. Add domains with this form, or select domains and move them into this group

Add Domains:

Add Domain(s)

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
 - Enable DNSSEC
 - Do this for ALL your domains
-
- Common mistakes:
 - DMARC needs SPF and/or 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:
 - **example.dk:**
v=sf1 include:spf-internal.example.dk
include:spf-external.example.dk -all
 - **spf-internal.example.dk:**
v=spf1 include:spf.protection.outlook.com
ip4:37.123.123.4 ip4:37.123.123.5 -all
 - **spf-external.example.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

Remember the feedback !



Slides and demos from the conference will be available at

<https://github.com/nordicinfrastructureconference/2022>

References #1

- SPF
 - <https://www.kitterman.com/spf/validate.html>
 - <https://www.spfwizard.net/>
- DKIM
 - <https://dkimvalidator.com/>
- DMARC
 - <https://mxtoolbox.com/dmarc.aspx>
 - <https://dmarcguide.globalcyberalliance.org/#/>

References #2

- Secure SMTP connections using TLS
 - <https://www.checktls.com/TestReceiver>
- Defender for Office 365
 - <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp>
- Mastering Configuration
 - <https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/mastering-configuration-in-defender-for-office-365-part-one/ba-p/2300064>
- User Adoption & Awareness Campaigns
 - <https://phishingquiz.withgoogle.com>