2022

Securing identities in Microsoft 365

Jan Bakker

JAN BAKKER consulting

2022

Jan Bakker

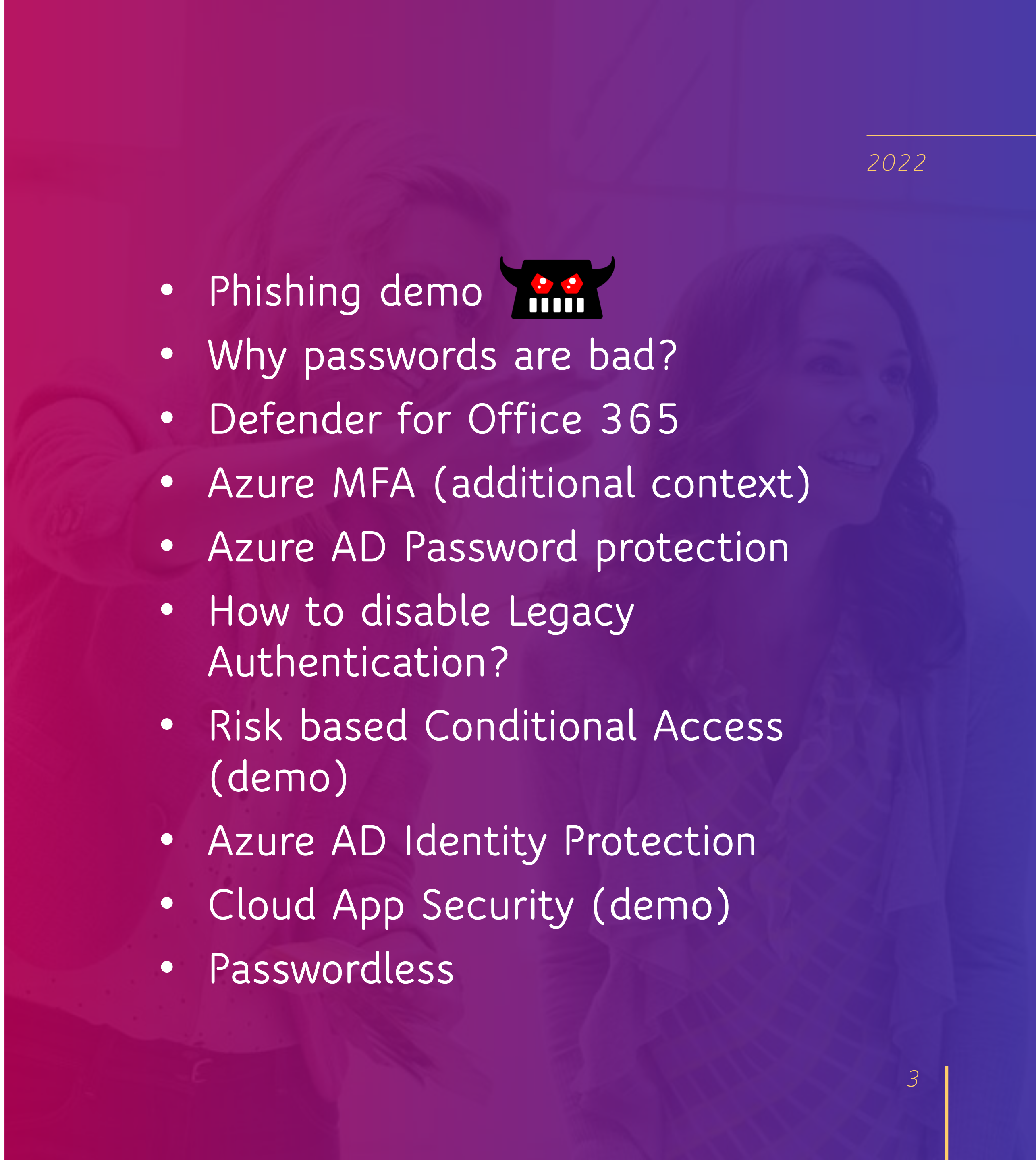
Microsoft 365 consultant

@janbakker_

MVP Microsoft® Most Valuable Professional

Agenda

What we will learn from today’s session



- Phishing demo
- Why passwords are bad?
- Defender for Office 365
- Azure MFA (additional context)
- Azure AD Password protection
- How to disable Legacy Authentication?
- Risk based Conditional Access (demo)
- Azure AD Identity Protection
- Cloud App Security (demo)
- Passwordless

“Identity is the new perimeter”

Zero Trust

Why passwords are bad?

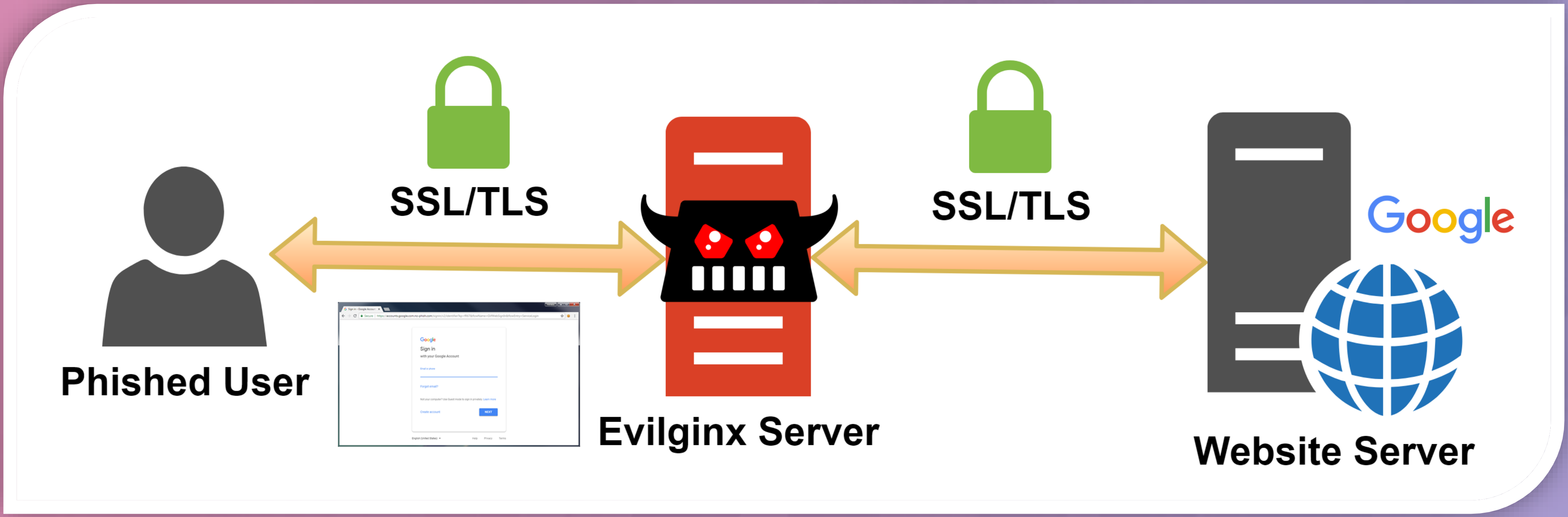
We cannot rely on passwords (alone)

- Humans are bad in making up good passwords
- Password re-use
- Passwords get stolen all the time
- Lack of Single Sign On = a gazillion passwords for day-to-day use
- Password reset policies make passwords weaker

Phishing demo

DEMO

2022



SSL/TLS

SSL/TLS

Phished User

Evilginx Server

Website Server

10 tips to increase identity security

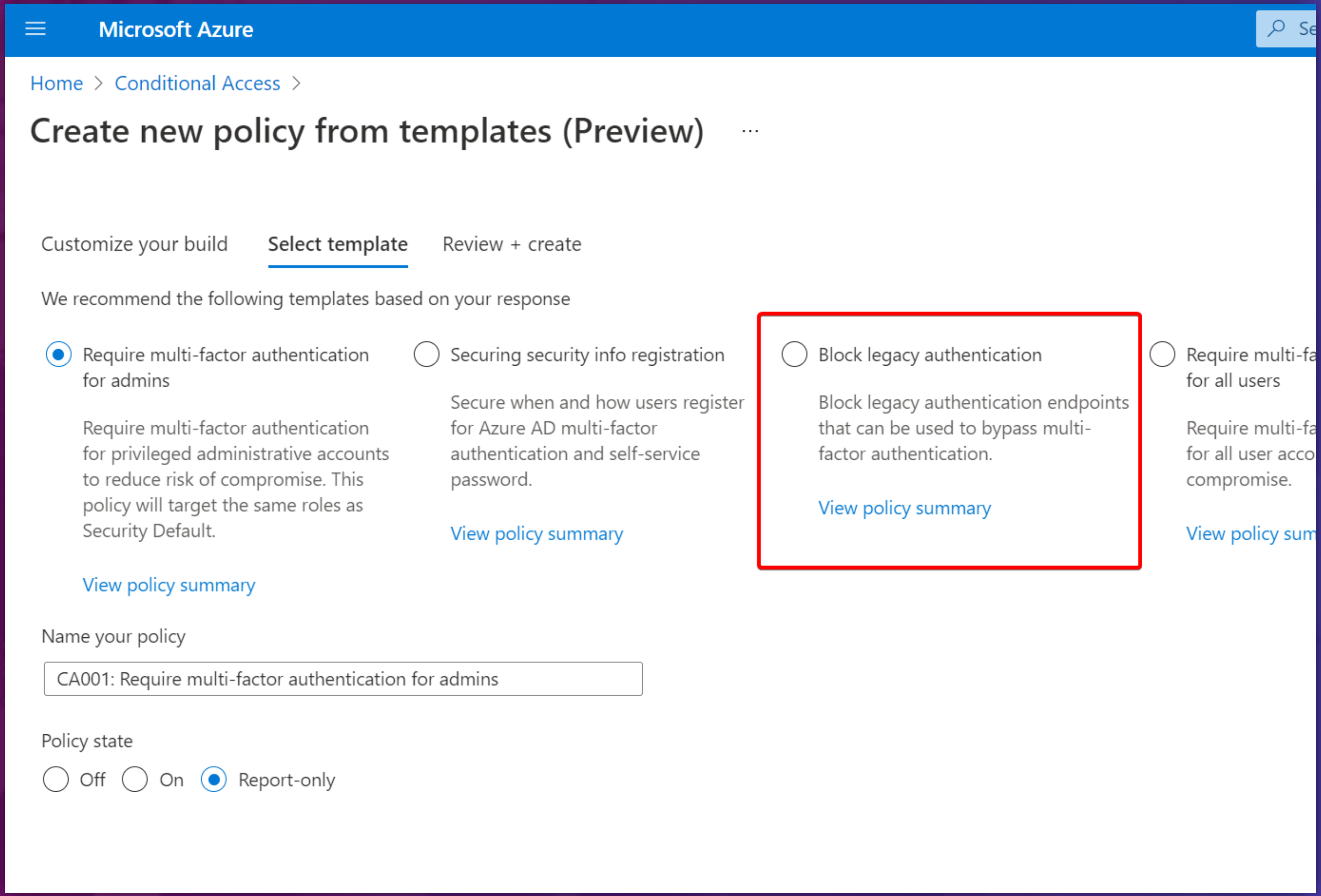
With Microsoft 365

TIP 1 – Block legacy authentication

Security Defaults

Conditional Access

DEMO



Home > Conditional Access >

Create new policy from templates (Preview) ...

Customize your build   Select template   Review + create

We recommend the following templates based on your response

● Require multi-factor authentication for admins

Require multi-factor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as Security Default.

View policy summary

○ Securing security info registration

Secure when and how users register for Azure AD multi-factor authentication and self-service password.

View policy summary

○ Block legacy authentication

Block legacy authentication endpoints that can be used to bypass multi-factor authentication.

View policy summary

○ Require multi-fa for all users

Require multi-fa for all user acco compromise.

View policy sum

Name your policy

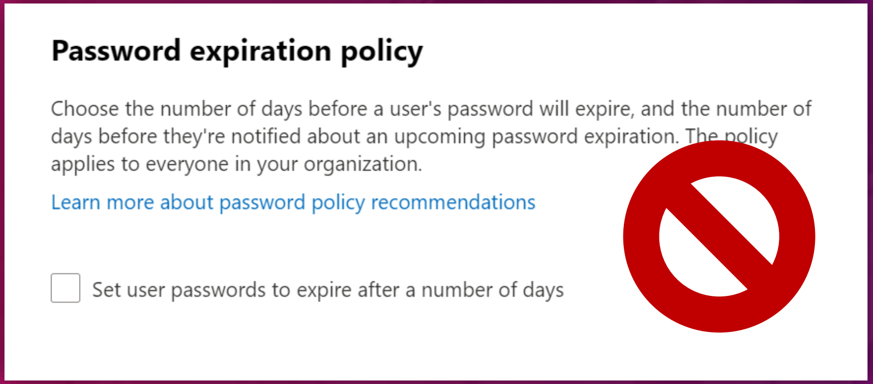
CA001: Require multi-factor authentication for admins

Policy state

○ Off ○ On ● Report-only

TIP 2 – Do not expire passwords

Use Azure AD password protection instead

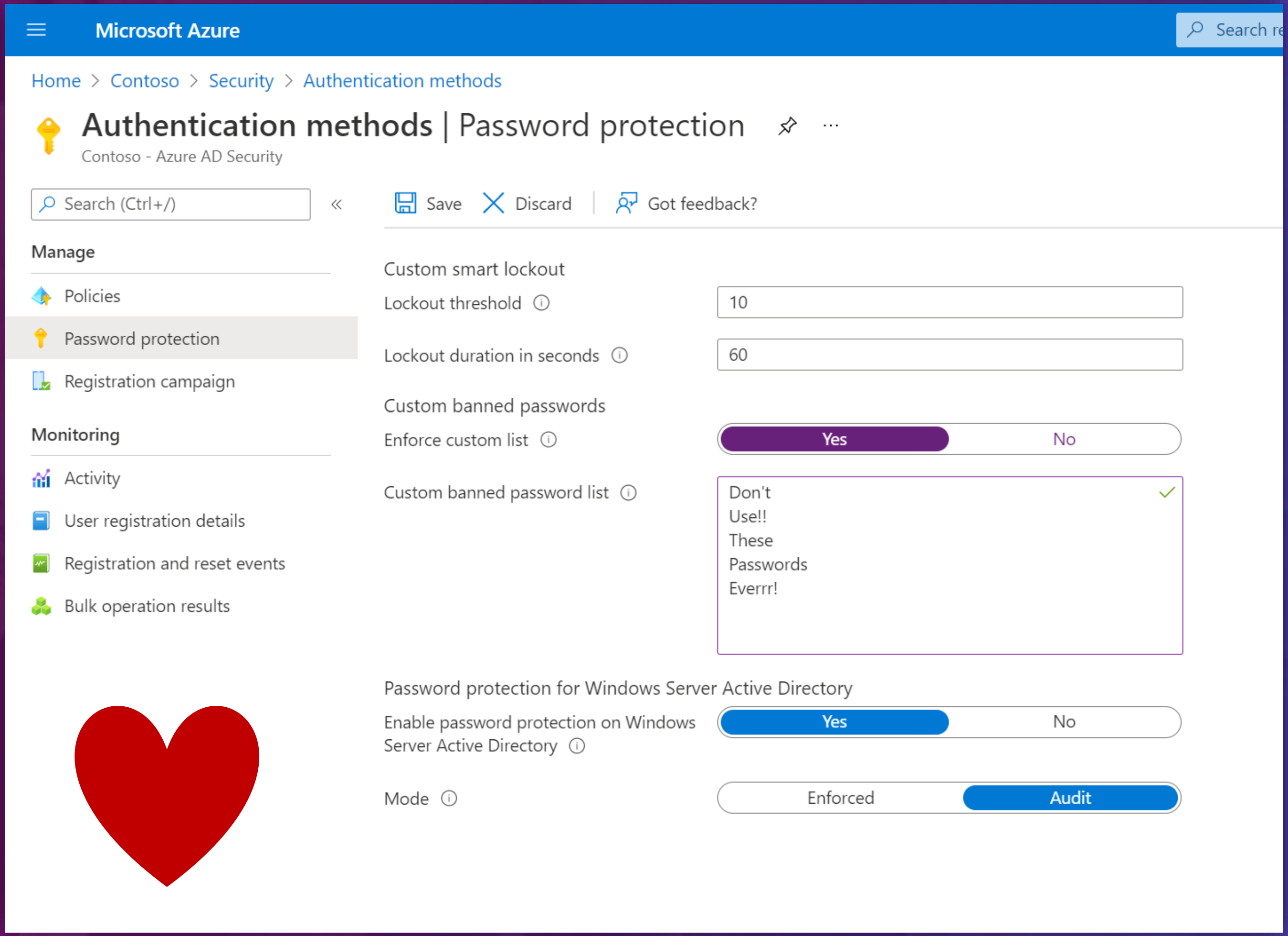


Password expiration policy

Choose the number of days before a user's password will expire, and the number of days before they're notified about an upcoming password expiration. The policy applies to everyone in your organization.

Learn more about password policy recommendations

□ Set user passwords to expire after a number of days



Home > Contoso > Security > Authentication methods

Authentication methods | Password protection

Contoso - Azure AD Security

Custom smart lockout

Lockout threshold: 10

Lockout duration in seconds: 60

Custom banned passwords

Enforce custom list: [✓ Yes] No

Custom banned password list:
Don't
Use!!
These
Passwords
Everrr!

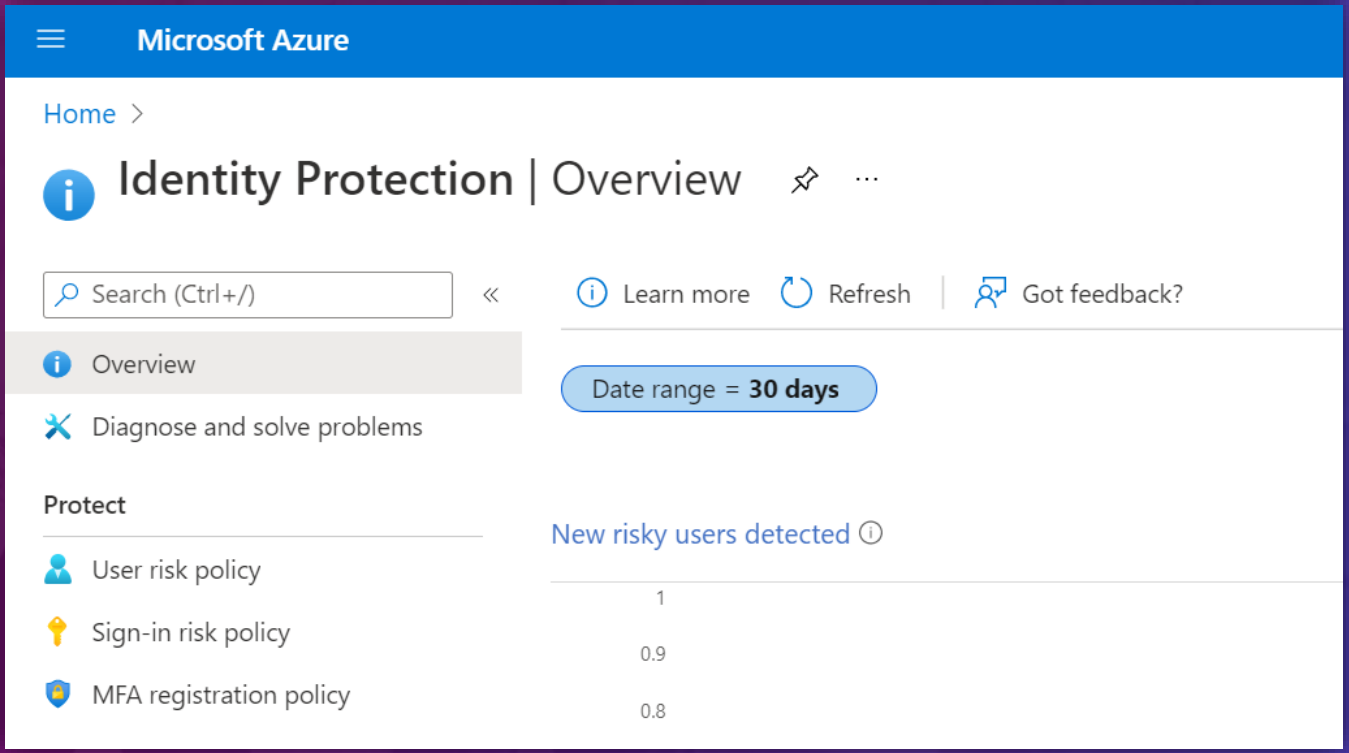
Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory: [✓ Yes] No

Mode: Enforced [✓ Audit]

TIP 3 – Turn on user risk / sign-in risk policy

- Azure AD Identity Protection
- Risk based Conditional Access
- Security Defaults



Microsoft Azure

Home >

Identity Protection | Overview

Search (Ctrl+/)

Learn more | Refresh | Got feedback?

Overview

Diagnose and solve problems

Protect

User risk policy

Sign-in risk policy

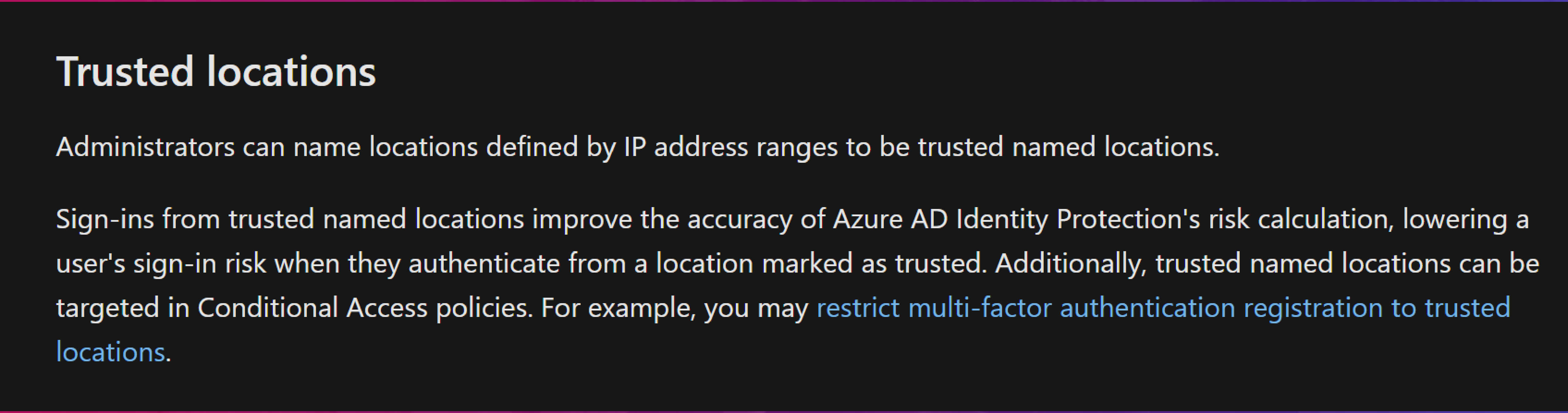
MFA registration policy

Date range = **30 days**

New risky users detected

DEMO

General tip: use Named/Trusted Locations to avoid false positives!



Trusted locations

Administrators can name locations defined by IP address ranges to be trusted named locations.

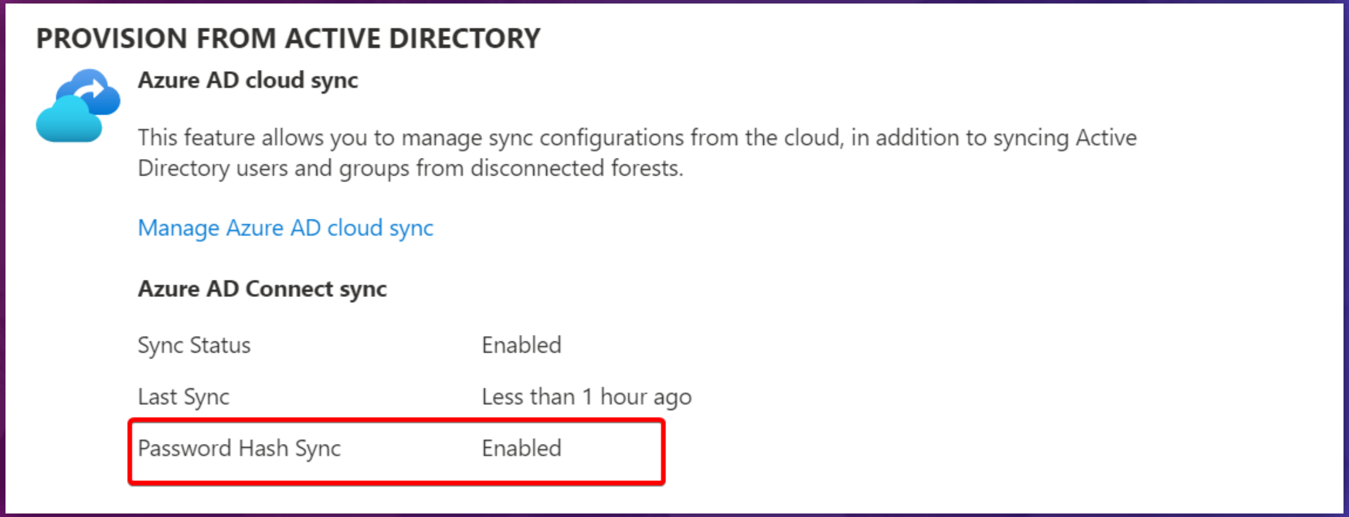
Sign-ins from trusted named locations improve the accuracy of Azure AD Identity Protection's risk calculation, lowering a user's sign-in risk when they authenticate from a location marked as trusted. Additionally, trusted named locations can be targeted in Conditional Access policies. For example, you may restrict multi-factor authentication registration to trusted locations.

TIP 4 – Enable password hash sync

- Leaked credentials detection for hybrid accounts

';--have i been pwned?

Check if your email or phone is in a data breach



PROVISION FROM ACTIVE DIRECTORY

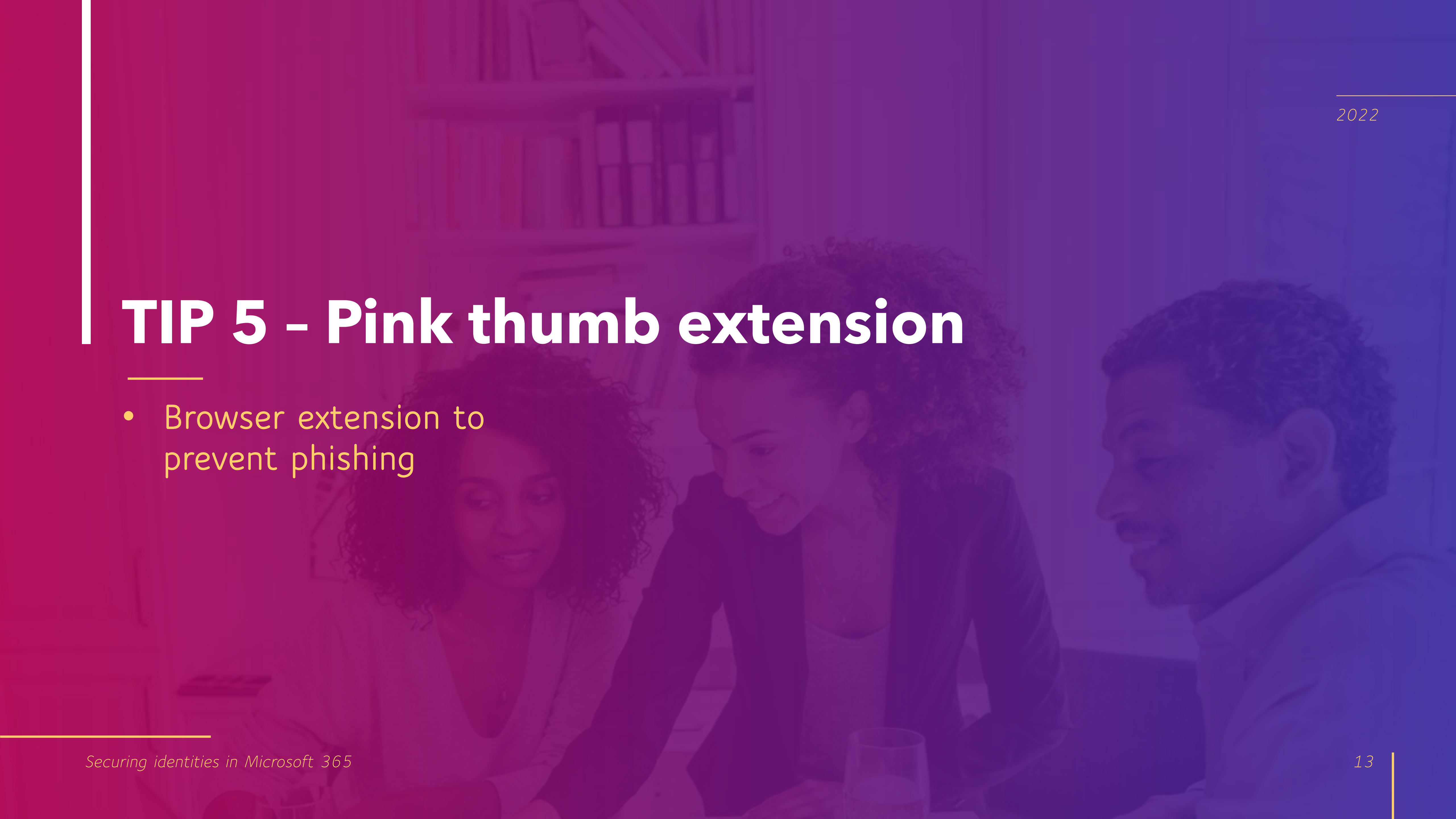
Azure AD cloud sync

This feature allows you to manage sync configurations from the cloud, in addition to syncing Active Directory users and groups from disconnected forests.

Manage Azure AD cloud sync

Azure AD Connect sync

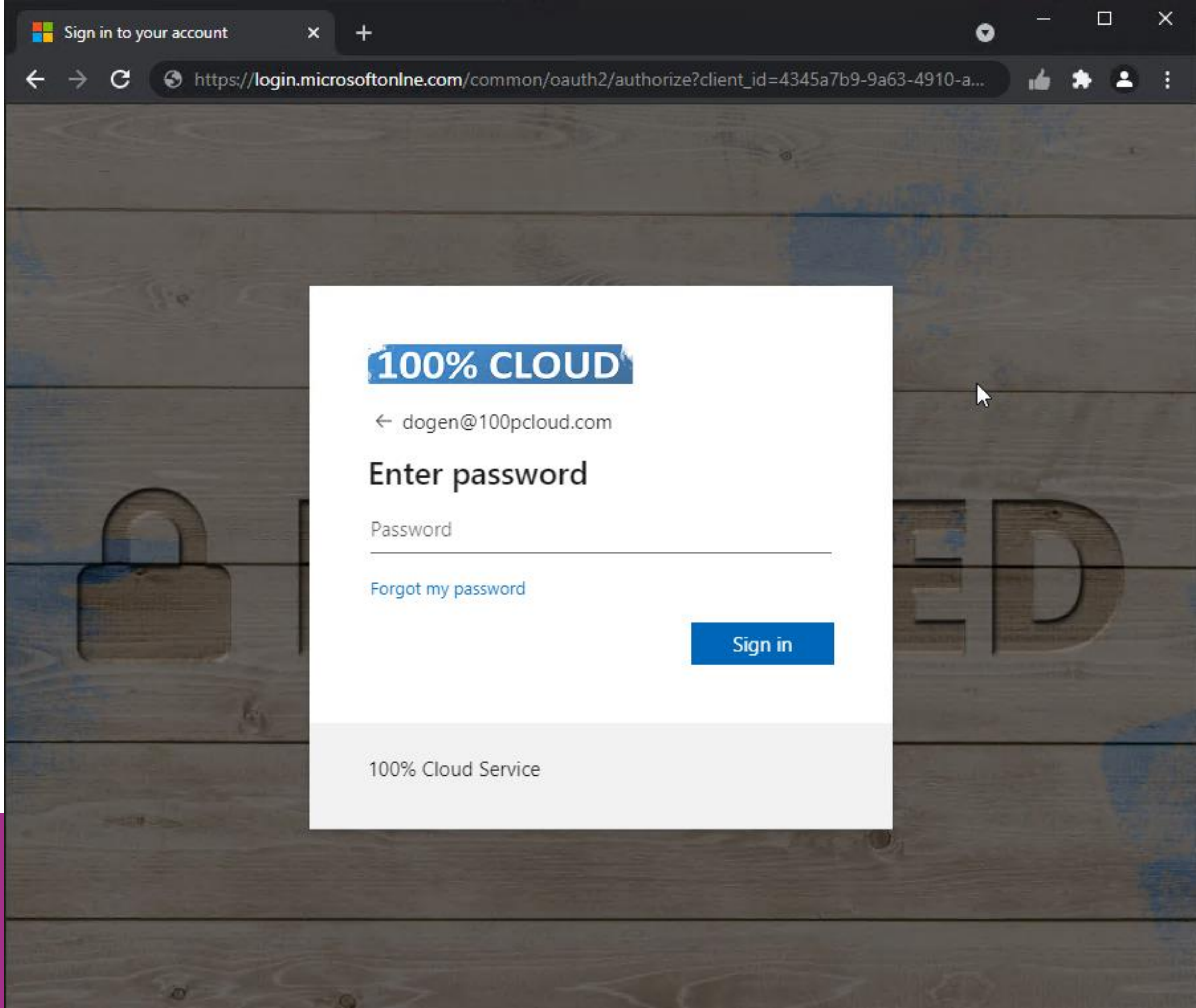
Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled



TIP 5 – Pink thumb extension

- Browser extension to prevent phishing

What's wrong with this page?



Sign in to your account

https://login.microsoftonlne.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a...

100% CLOUD

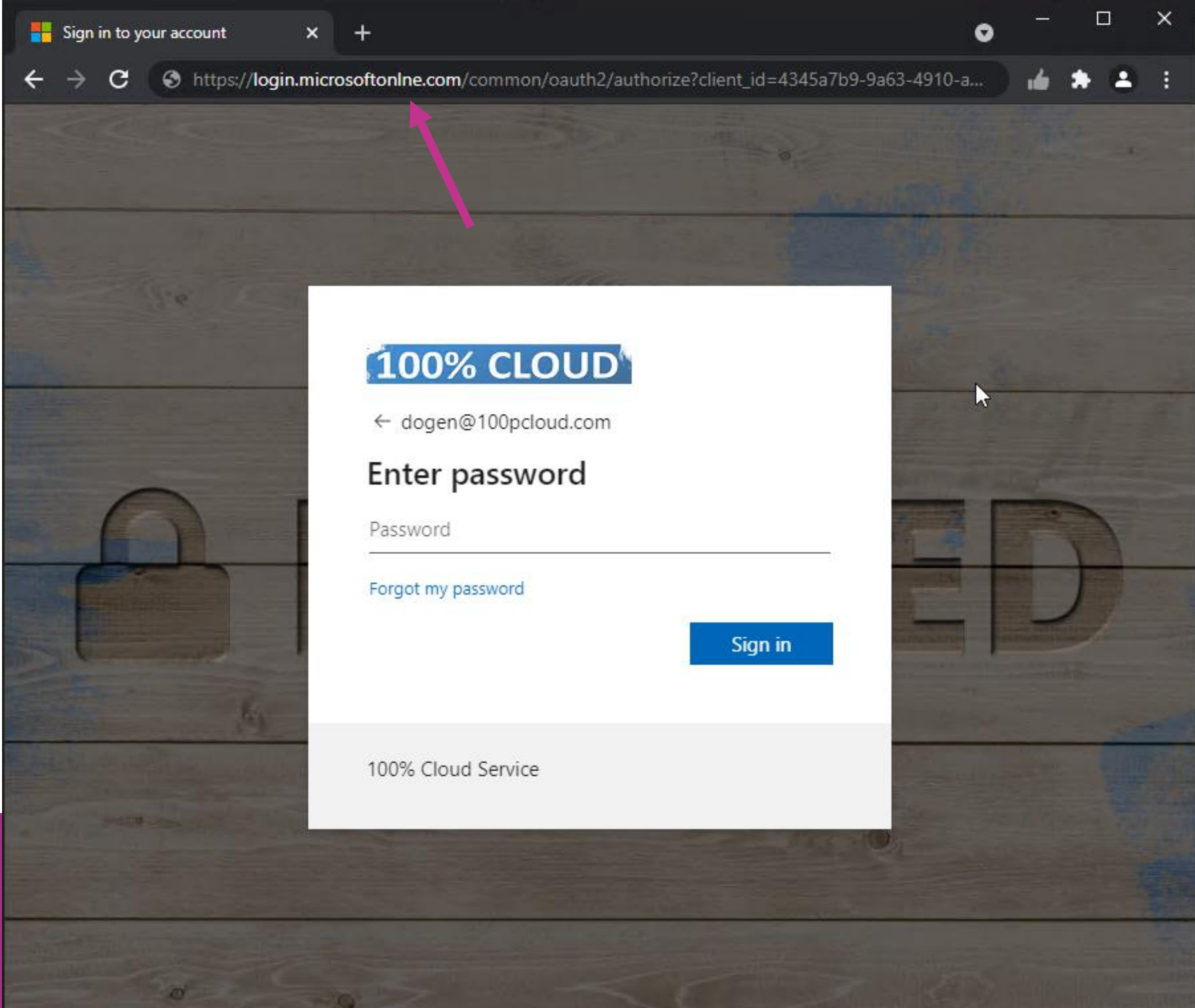
dogen@100pcloud.com

Enter password

Password

100% Cloud Service

What's wrong with this page?



https://login.microsoftonlne.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a...

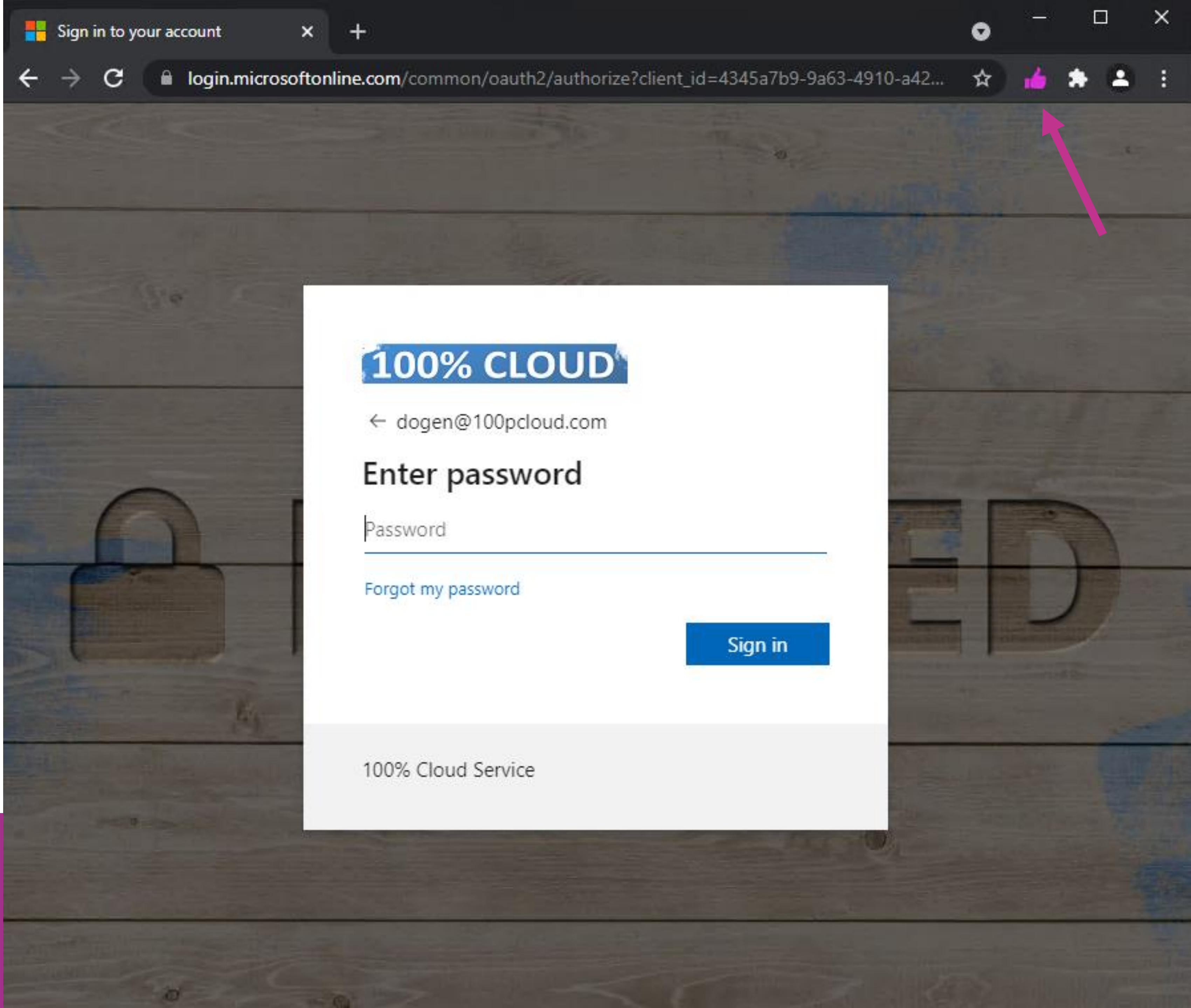
← dogen@100pcloud.com

Enter password

Password

100% Cloud Service

Can you see the pink thumb icon?



Sign in to your account

login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a42...

100% CLOUD

← dogen@100pcloud.com

Enter password

Password

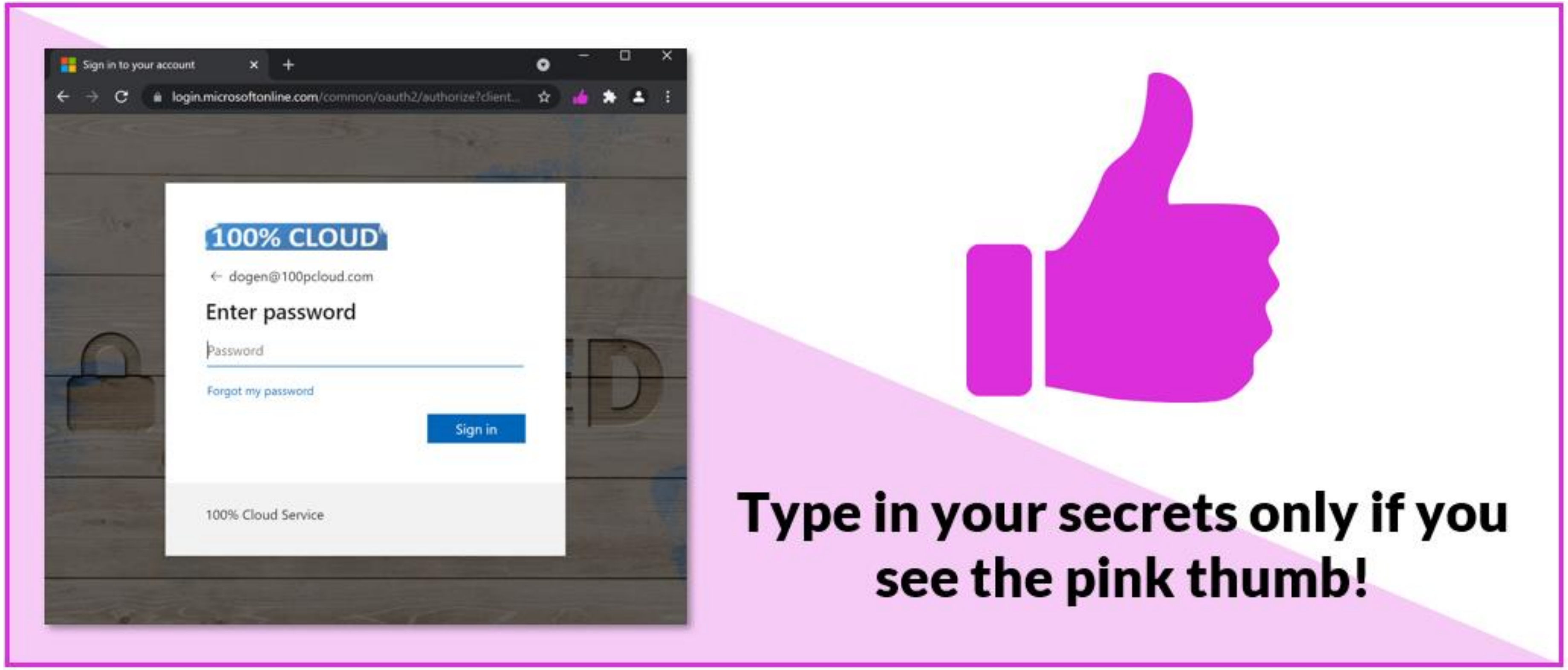
Forgot my password

Sign in

100% Cloud Service

PINK THUMB

Pink Thumb | (emptydc.com)



Sign in to your account

login.microsoftonline.com/common/oauth2/authorize?client...

100% CLOUD

dogen@100pcloud.com

Enter password

Password

Forgot my password

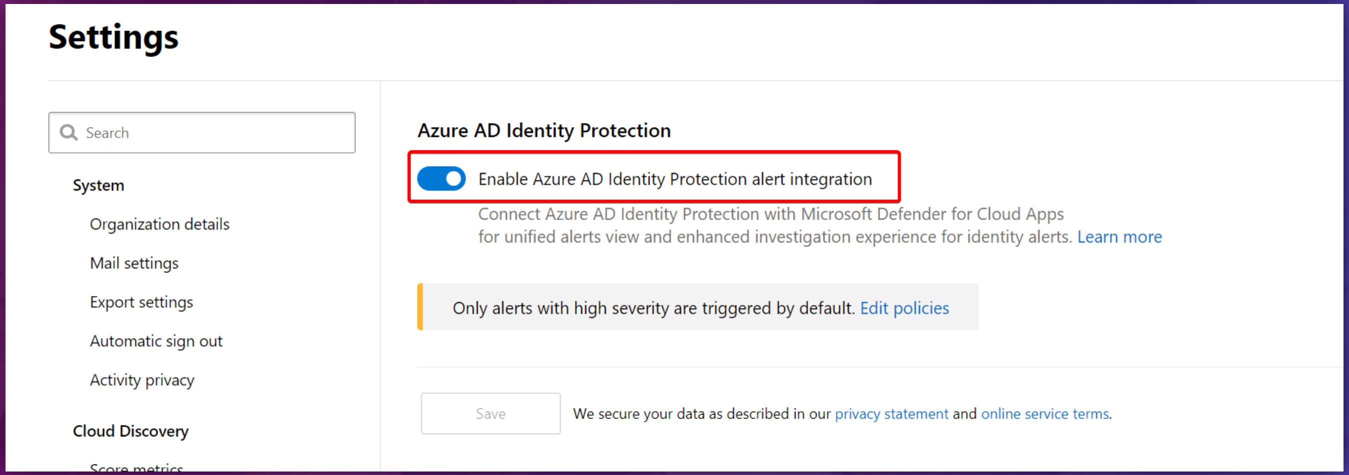
Sign in

100% Cloud Service

Type in your secrets only if you see the pink thumb!

TIP 6 – Defender for Cloud Apps

- Integration with Identity Protection



Settings

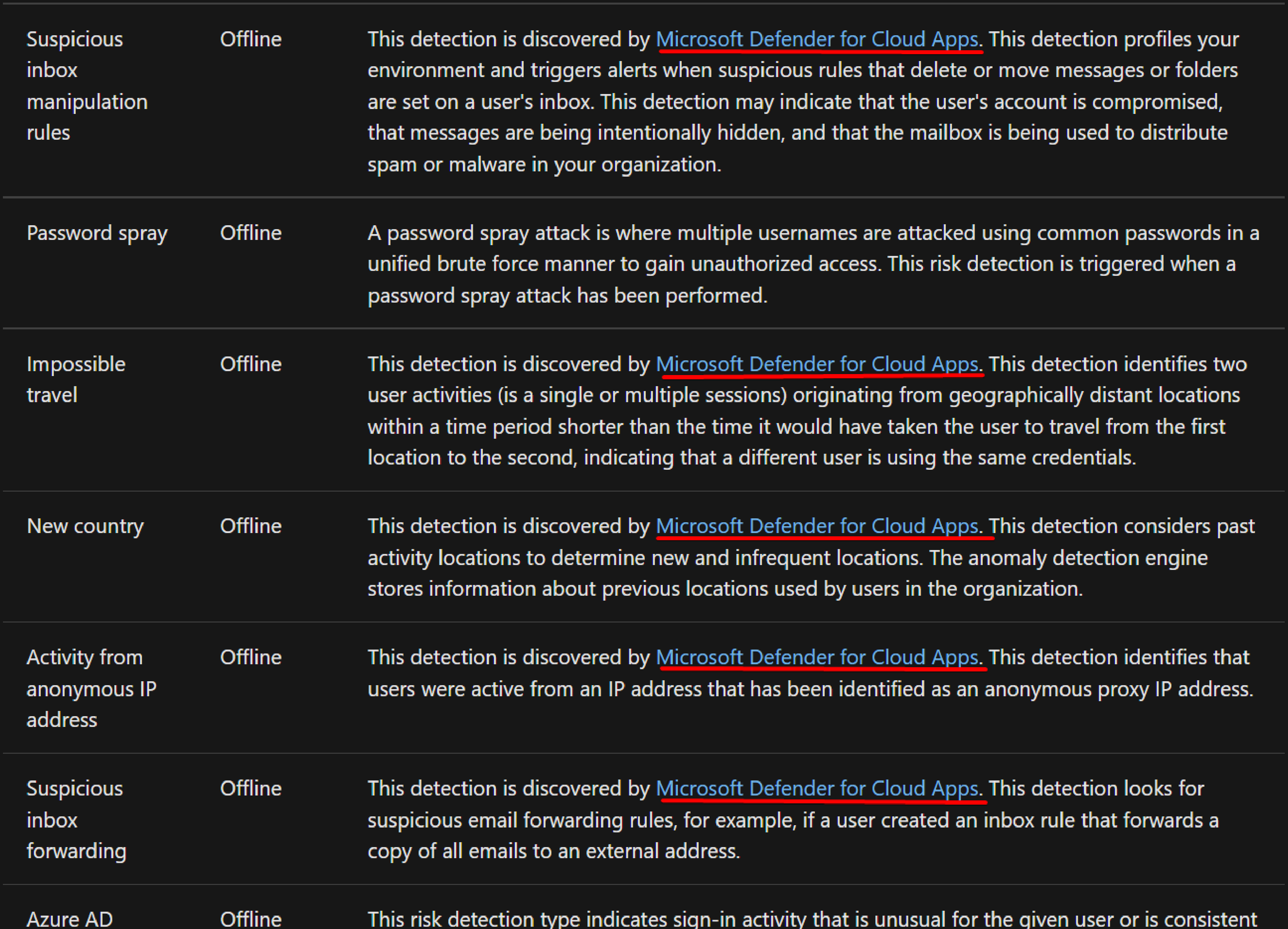
Azure AD Identity Protection

● Enable Azure AD Identity Protection alert integration

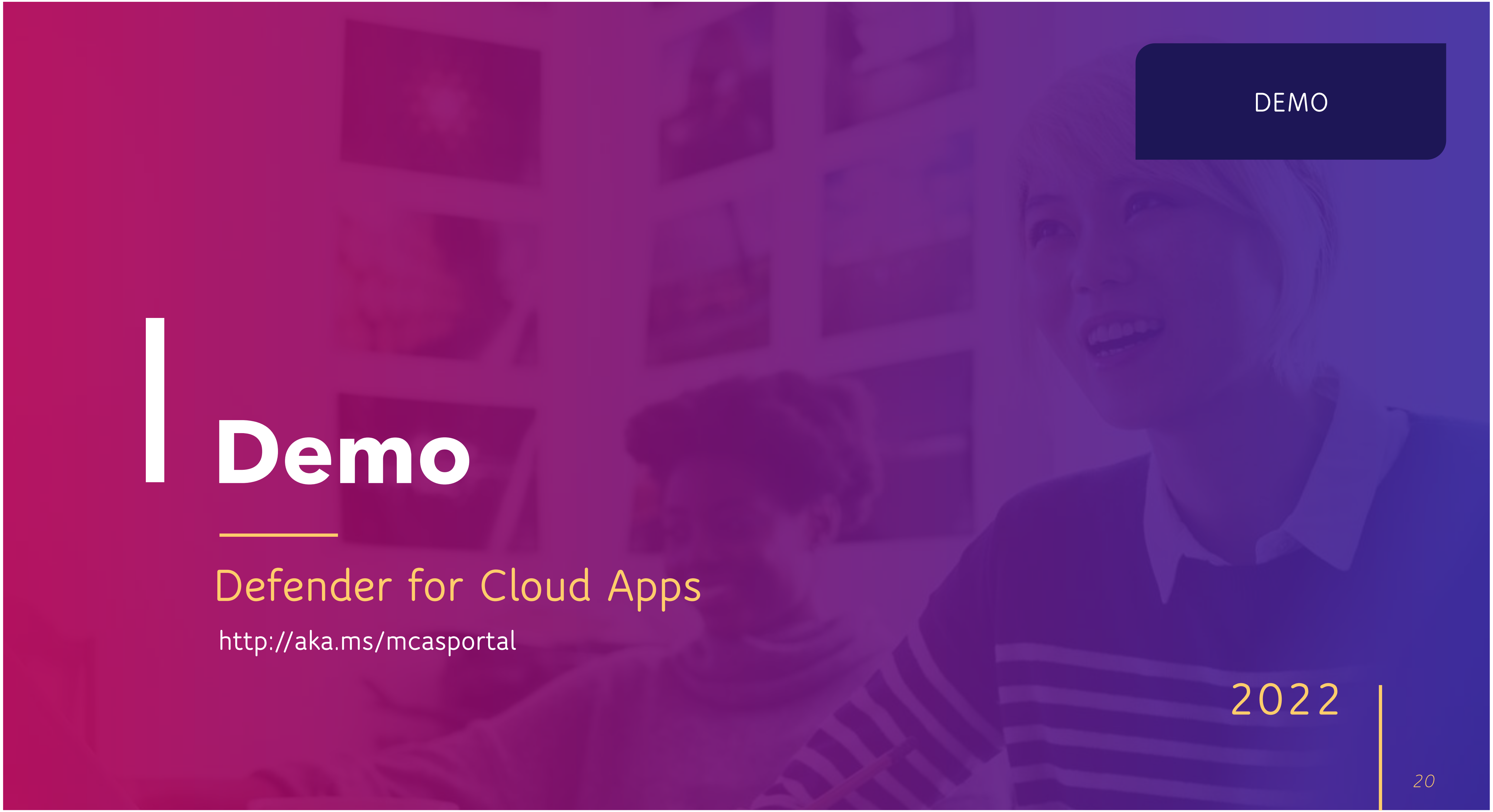
Connect Azure AD Identity Protection with Microsoft Defender for Cloud Apps for unified alerts view and enhanced investigation experience for identity alerts. Learn more

Only alerts with high severity are triggered by default. Edit policies

We secure your data as described in our privacy statement and online service terms.



Suspicious inbox manipulation rules	Offline	This detection is discovered by Microsoft Defender for Cloud Apps. This detection profiles your environment and triggers alerts when suspicious rules that delete or move messages or folders are set on a user's inbox. This detection may indicate that the user's account is compromised, that messages are being intentionally hidden, and that the mailbox is being used to distribute spam or malware in your organization.
Password spray	Offline	A password spray attack is where multiple usernames are attacked using common passwords in a unified brute force manner to gain unauthorized access. This risk detection is triggered when a password spray attack has been performed.
Impossible travel	Offline	This detection is discovered by Microsoft Defender for Cloud Apps. This detection identifies two user activities (is a single or multiple sessions) originating from geographically distant locations within a time period shorter than the time it would have taken the user to travel from the first location to the second, indicating that a different user is using the same credentials.
New country	Offline	This detection is discovered by Microsoft Defender for Cloud Apps. This detection considers past activity locations to determine new and infrequent locations. The anomaly detection engine stores information about previous locations used by users in the organization.
Activity from anonymous IP address	Offline	This detection is discovered by Microsoft Defender for Cloud Apps. This detection identifies that users were active from an IP address that has been identified as an anonymous proxy IP address.
Suspicious inbox forwarding	Offline	This detection is discovered by Microsoft Defender for Cloud Apps. This detection looks for suspicious email forwarding rules, for example, if a user created an inbox rule that forwards a copy of all emails to an external address.
Azure AD	Offline	This risk detection type indicates sign-in activity that is unusual for the given user or is consistent



DEMO

Demo

Defender for Cloud Apps

http://aka.ms/mcasportal

2022

TIP 7 – Azure MFA additional context & Sign-in frequency

- Avoid MFA fatigue and mindless approvals of pop-ups.

Can we prompt our users with MFA every 8 hours, or even better: every single time they sign-on?

Azure AD Multi-Factor Authentication prompts and session lifetime | Microsoft Docs

2022

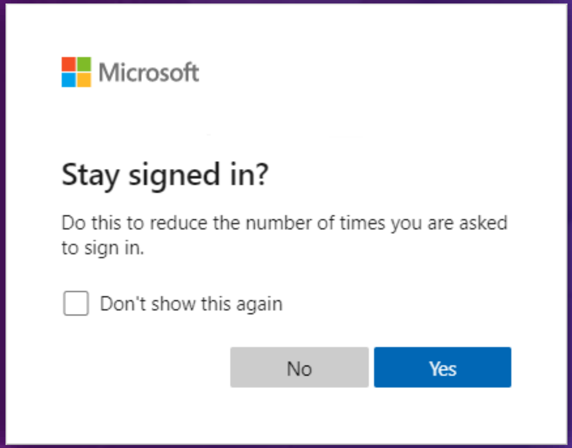
Azure AD premium

- Enable Seamless SSO
- Use Sign-in frequency (Conditional Access) if you require reauthentication
- Non managed = non persistent, or: less risk = longer session duration

Don’t use both!

Azure AD free

- Enable Seamless SSO
- Keep the Remain signed-in option enabled, and guide your users to accept it.



Microsoft

Stay signed in?

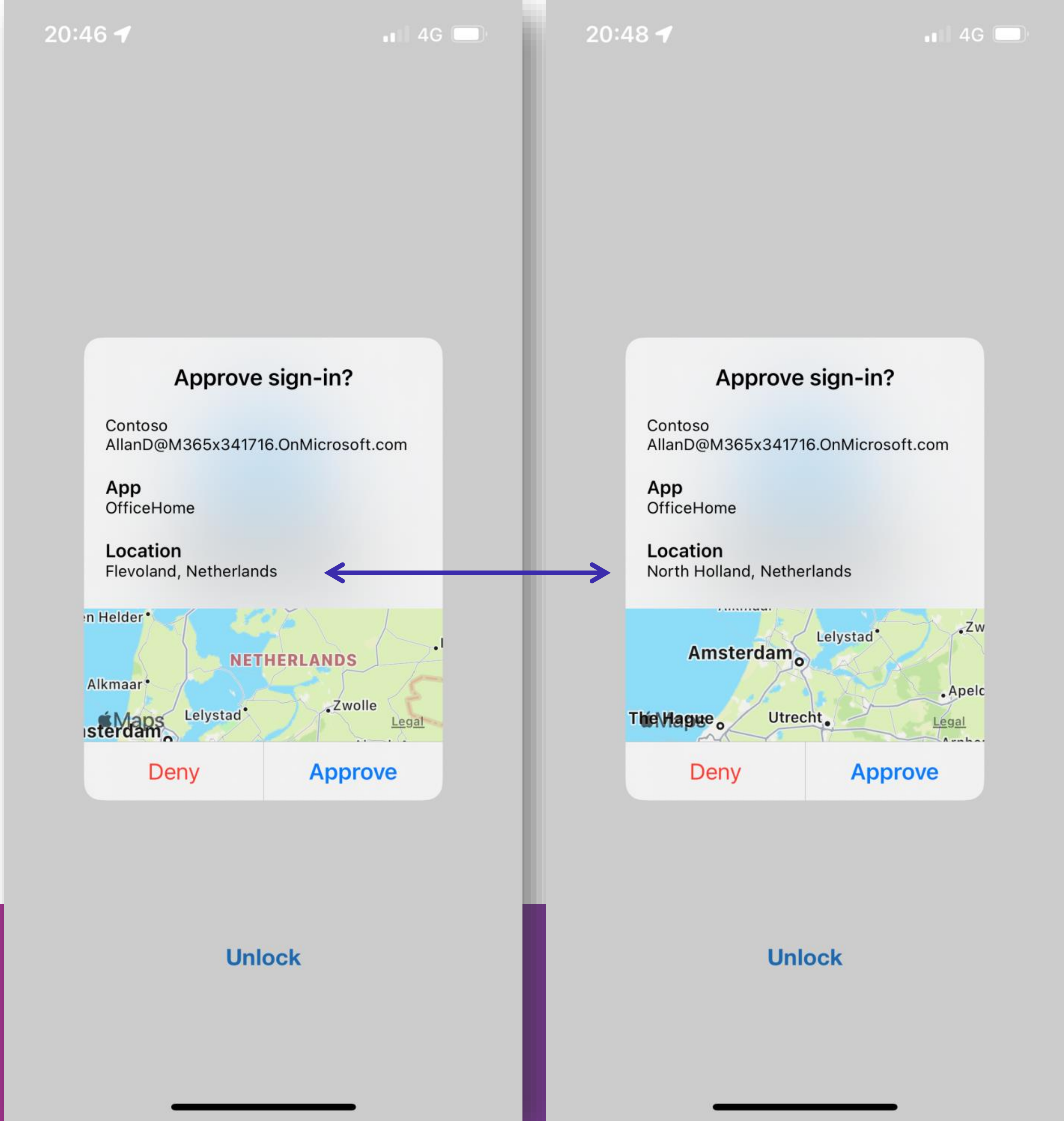
Do this to reduce the number of times you are asked to sign in.

☐ Don't show this again

No Yes

Additional Context in Azure MFA notifications

DEMO



20:46 4G

Approve sign-in?

Contoso
AllanD@M365x341716.OnMicrosoft.com

App
OfficeHome

Location
Flevoland, Netherlands

Deny | Approve

Unlock

20:48 4G

Approve sign-in?

Contoso
AllanD@M365x341716.OnMicrosoft.com

App
OfficeHome

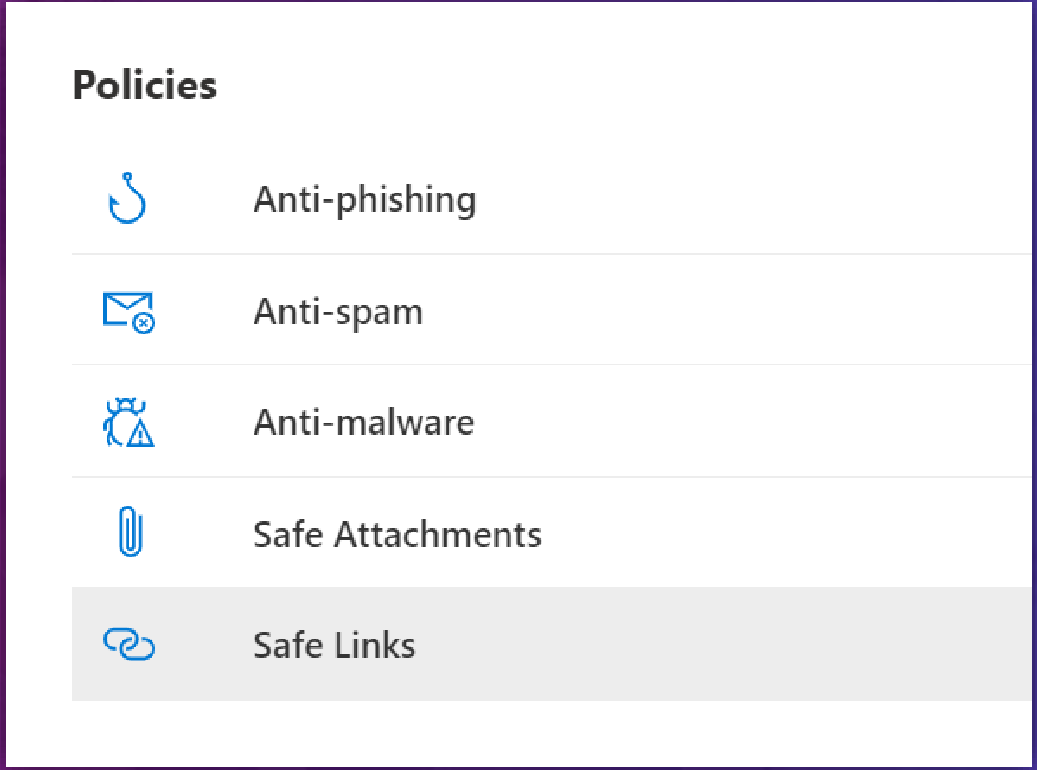
Location
North Holland, Netherlands

Deny | Approve

Unlock

TIP 8 – Defender for Office 365

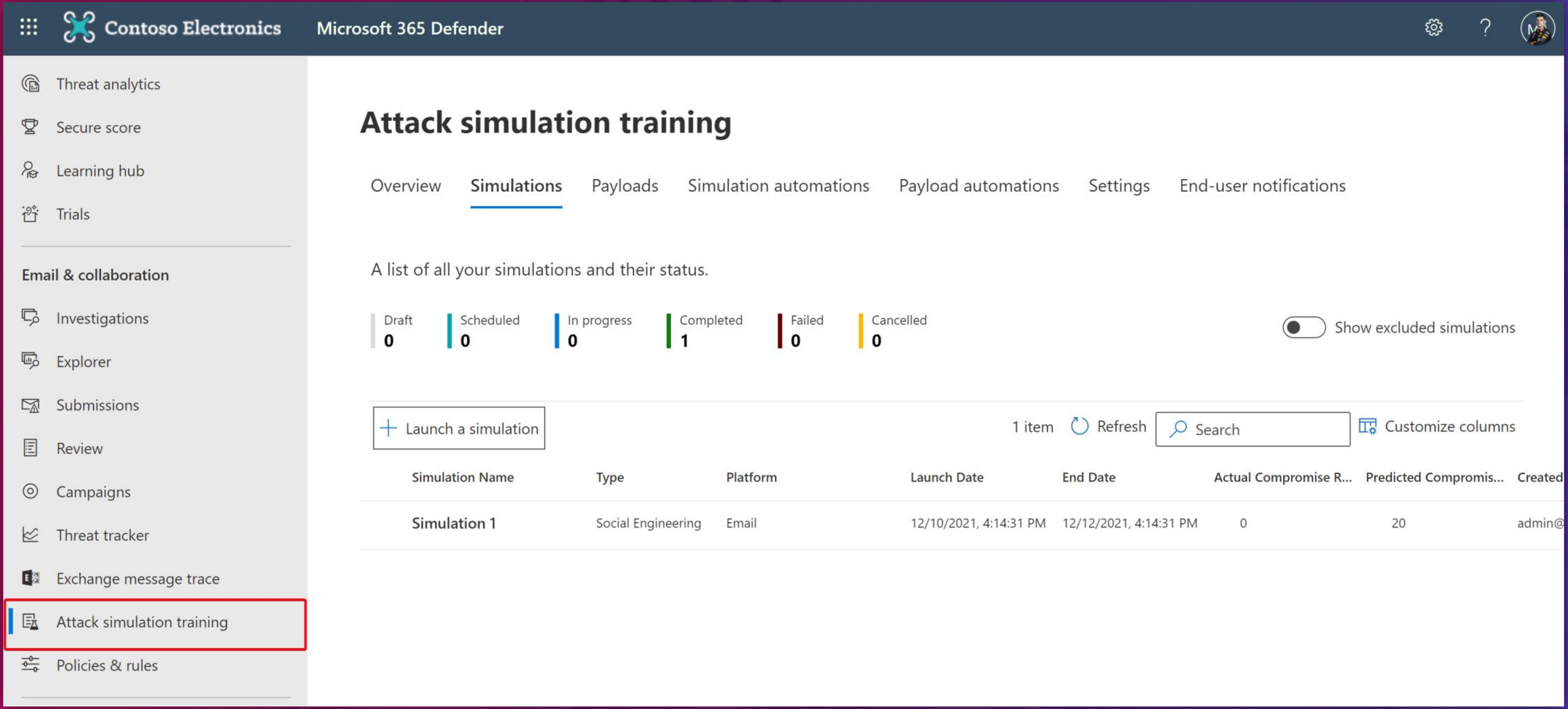
- Attack Simulator
- Smart Links
- Anti phishing policies



Policies

- Anti-phishing
- Anti-spam
- Anti-malware
- Safe Attachments
- Safe Links

Attack simulation training in Defender for Office 365



Attack simulation training

A list of all your simulations and their status.

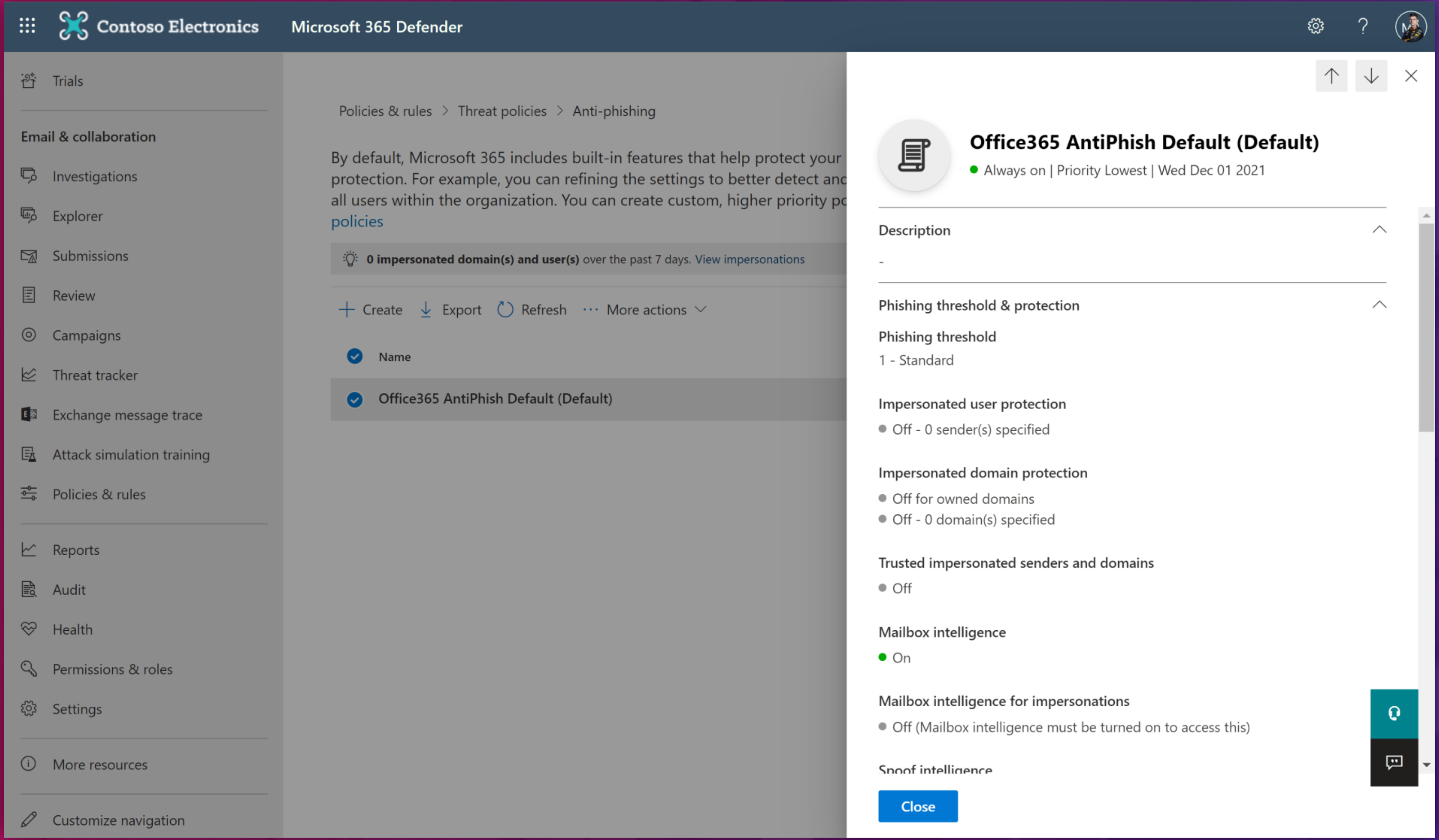
Draft	Scheduled	In progress	Completed	Failed	Cancelled
0	0	0	1	0	0

Simulation Name	Type	Platform	Launch Date	End Date	Actual Compromise R...	Predicted Compromis...	Created
Simulation 1	Social Engineering	Email	12/10/2021, 4:14:31 PM	12/12/2021, 4:14:31 PM	0	20	admin@

Educate your users

Congratulations on never being caught in a phishing campaign
Me who never reads emails
meme-arsenal.ru

Anti-phishing



Policies & rules > Threat policies > Anti-phishing

By default, Microsoft 365 includes built-in features that help protect your
protection. For example, you can refining the settings to better detect and
all users within the organization. You can create custom, higher priority po
policies

0 impersonated domain(s) and user(s) over the past 7 days. View impersonations

Name

Office365 AntiPhish Default (Default)

Office365 AntiPhish Default (Default)

Always on | Priority Lowest | Wed Dec 01 2021

Description

-

Phishing threshold & protection

Phishing threshold

1 - Standard

Impersonated user protection

- Off - 0 sender(s) specified

Impersonated domain protection

- Off for owned domains
- Off - 0 domain(s) specified

Trusted impersonated senders and domains

- Off

Mailbox intelligence

- On

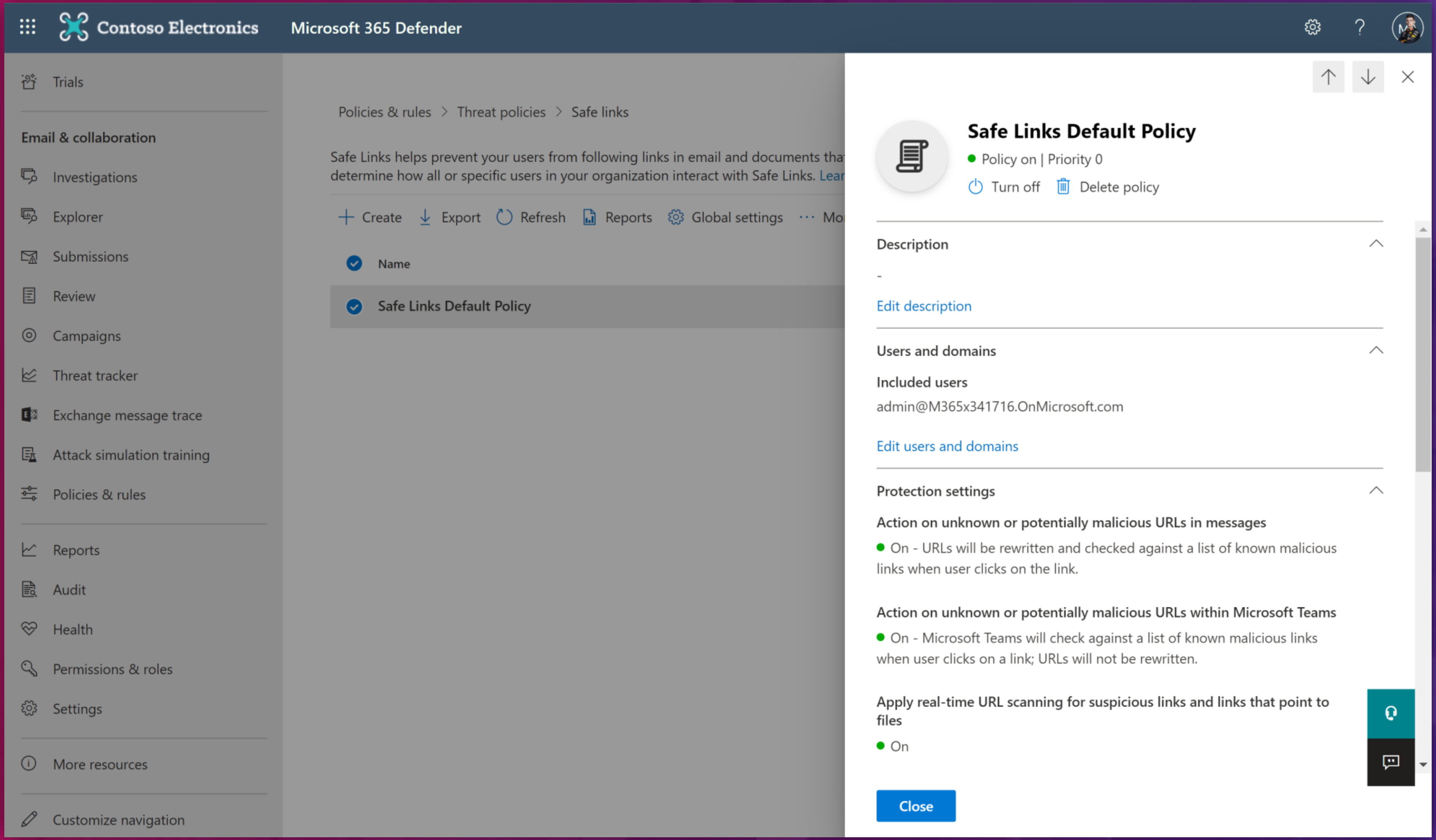
Mailbox intelligence for impersonations

- Off (Mailbox intelligence must be turned on to access this)

Spoof intelligence

Educate your users

Safe links



Safe Links helps prevent your users from following links in email and documents tha
determine how all or specific users in your organization interact with Safe Links. Lear

Safe Links Default Policy

Safe Links Default Policy

● Policy on | Priority 0

Description

-

Users and domains

Included users

admin@M365x341716.OnMicrosoft.com

Protection settings

Action on unknown or potentially malicious URLs in messages

● On - URLs will be rewritten and checked against a list of known malicious links when user clicks on the link.

Action on unknown or potentially malicious URLs within Microsoft Teams

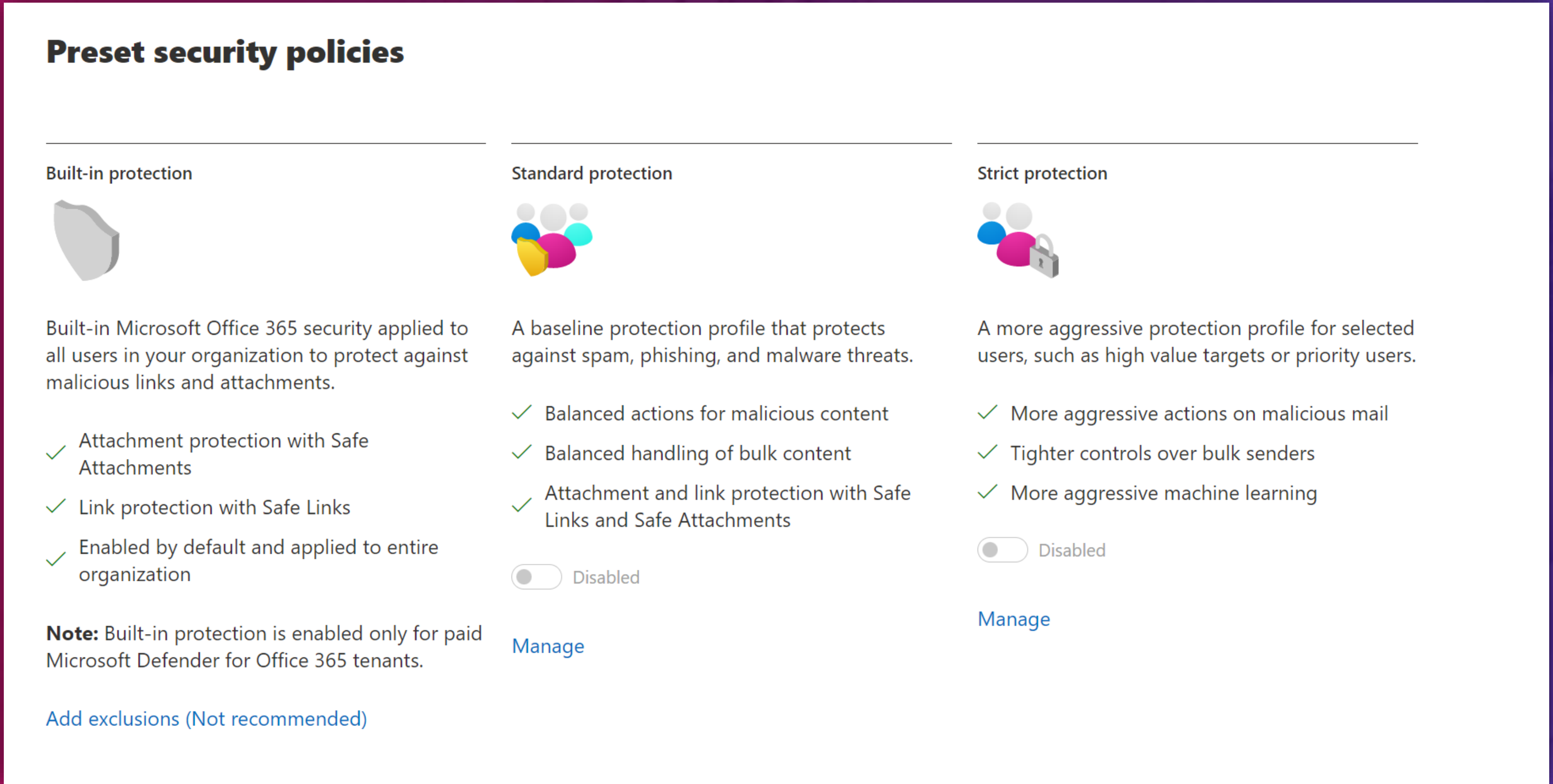
● On - Microsoft Teams will check against a list of known malicious links when user clicks on a link; URLs will not be rewritten.

Apply real-time URL scanning for suspicious links and links that point to files

● On

For Exchange Online and Teams!

Preset security 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.

- ✓ Attachment protection with Safe Attachments
- ✓ Link protection with Safe Links
- ✓ Enabled by default and applied to entire organization

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

Disabled

Manage

Strict protection

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

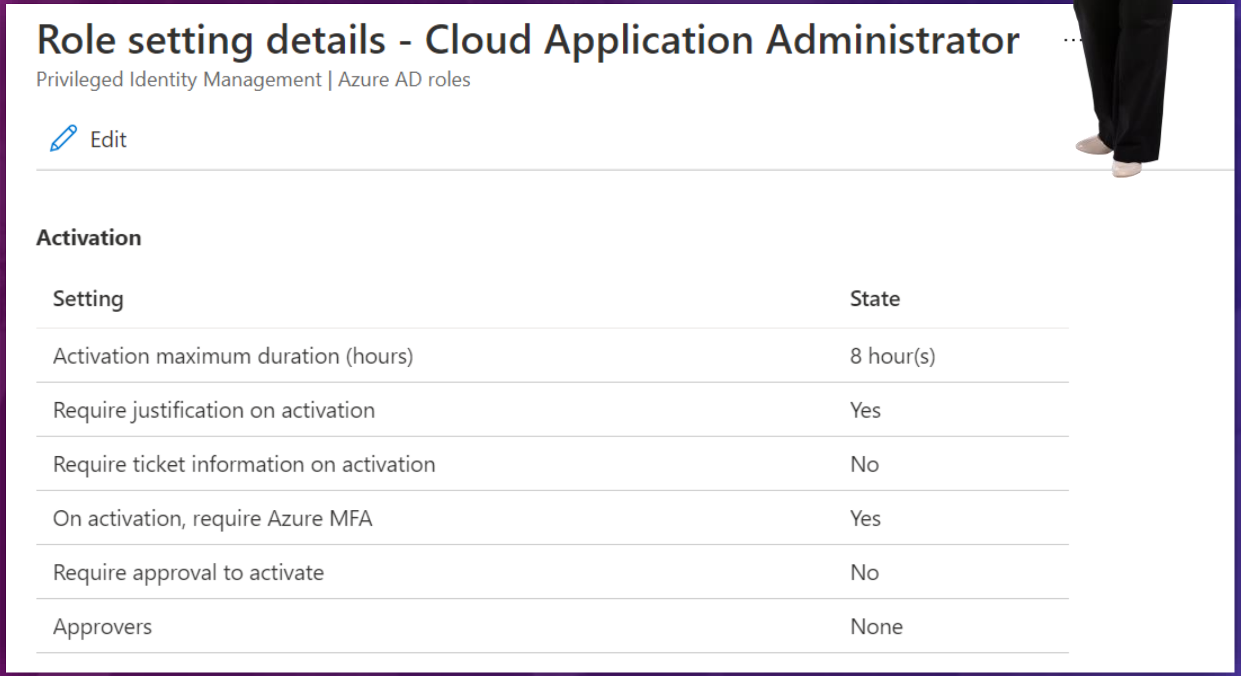
- ✓ More aggressive actions on malicious mail
- ✓ Tighter controls over bulk senders
- ✓ More aggressive machine learning

Disabled

Manage

TIP 9 – Privileged Identity Management

- Reduce standing access for admin roles
- MFA and approval before role is activated
- Access Reviews



Role setting details - Cloud Application Administrator

Privileged Identity Management | Azure AD roles

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	No
Approvers	None

Practice what you preach! Start out with your personal Microsoft account!

TIP 10 – Go Passwordless!

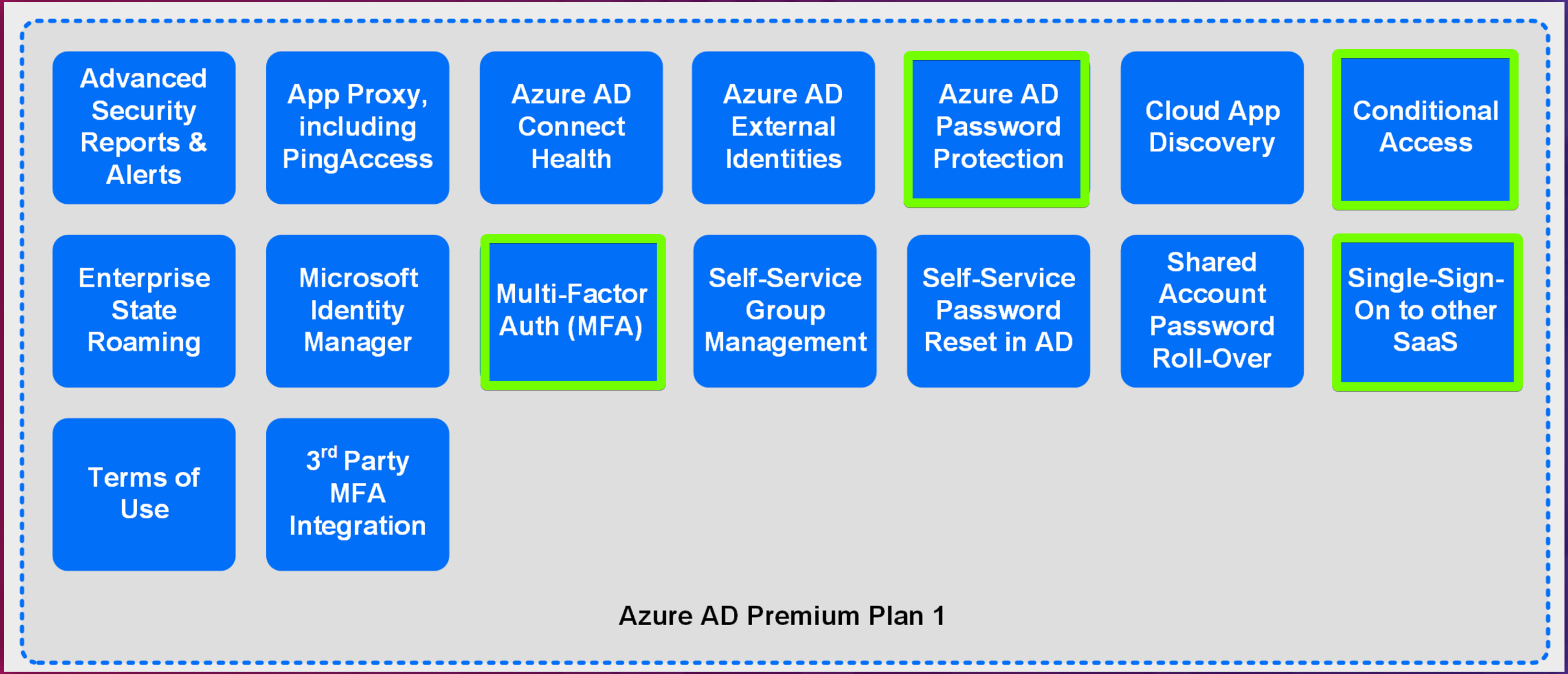
[The passwordless future is here for your Microsoft account - Microsoft Security Blog]

- Windows Hello for Business
- Microsoft Authenticator App
- FIDO 2 keys

DEMO

Enable Combined Registration portal first!

Azure AD Premium Plan 1



Advanced Security Reports & Alerts

App Proxy, including PingAccess

Azure AD Connect Health

Azure AD External Identities

Azure AD Password Protection

Cloud App Discovery

Conditional Access

Enterprise State Roaming

Microsoft Identity Manager

Multi-Factor Auth (MFA)

Self-Service Group Management

Self-Service Password Reset in AD

Shared Account Password Roll-Over

Single-Sign-On to other SaaS

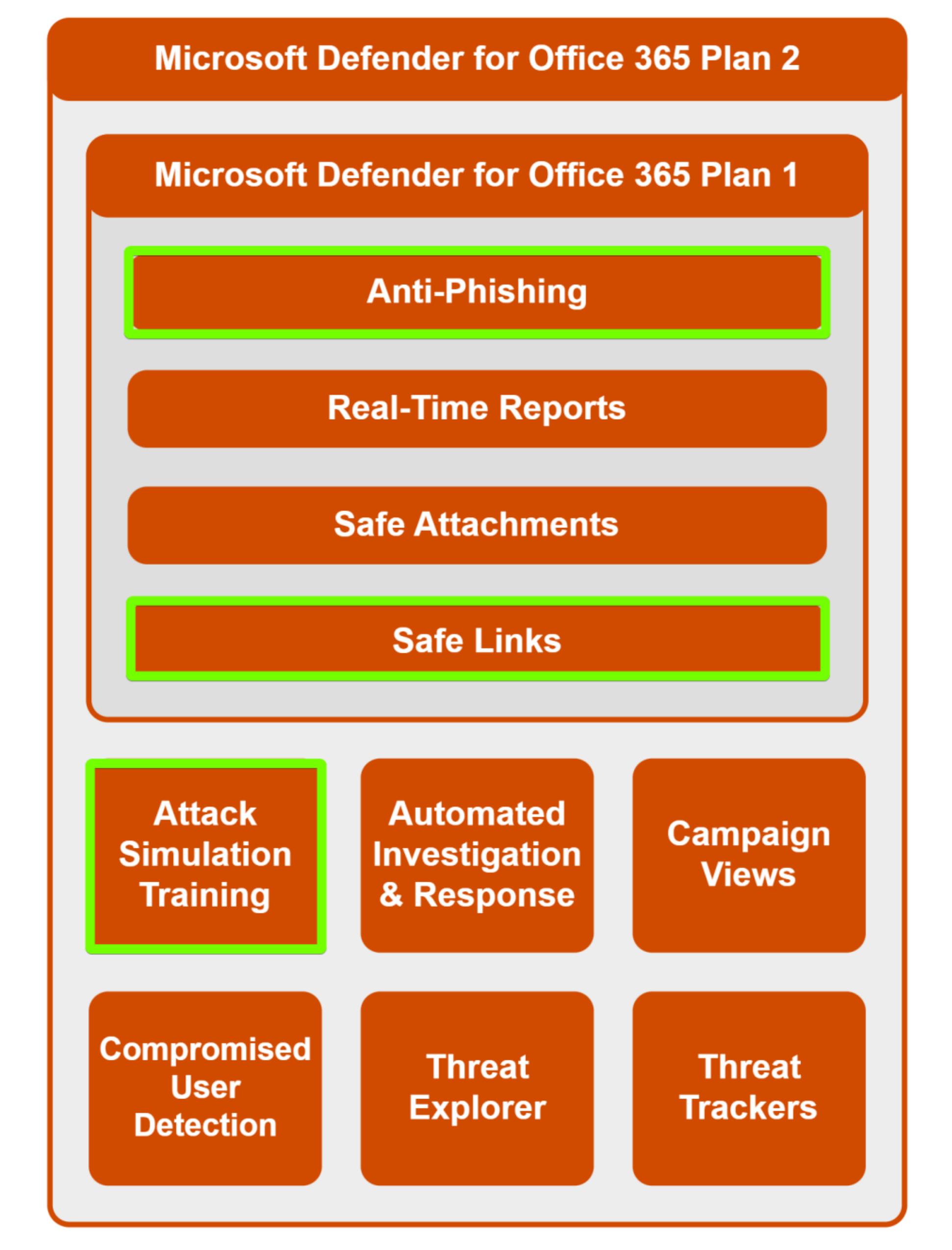
Terms of Use

3rd Party MFA Integration

Azure AD Premium Plan 1

EMS Enterprise E3 | M365 Maps

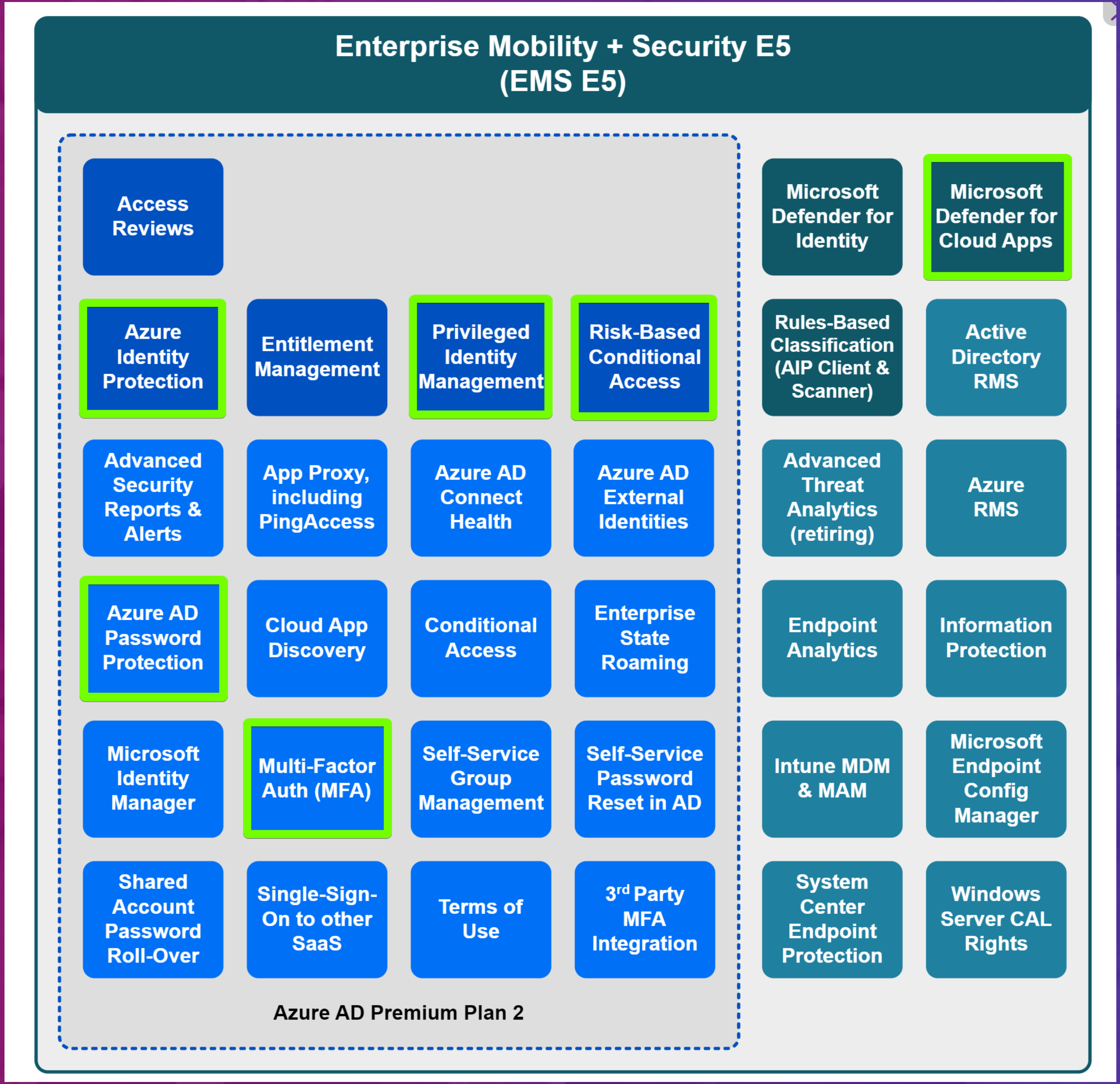
Prevent phishing



Microsoft Defender for Office 365 Plan 2
Microsoft Defender for Office 365 Plan 1
Anti-Phishing
Real-Time Reports
Safe Attachments
Safe Links
Attack Simulation Training
Automated Investigation & Response
Campaign Views
Compromised User Detection
Threat Explorer
Threat Trackers

Microsoft Defender for Office 365 | M365 Maps

Security & Alerts



Enterprise Mobility + Security E5 (EMS E5)

Access Reviews				Microsoft Defender for Identity	Microsoft Defender for Cloud Apps
Azure Identity Protection	Entitlement Management	Privileged Identity Management	Risk-Based Conditional Access	Rules-Based Classification (AIP Client & Scanner)	Active Directory RMS
Advanced Security Reports & Alerts	App Proxy, including PingAccess	Azure AD Connect Health	Azure AD External Identities	Advanced Threat Analytics (retiring)	Azure RMS
Azure AD Password Protection	Cloud App Discovery	Conditional Access	Enterprise State Roaming	Endpoint Analytics	Information Protection
Microsoft Identity Manager	Multi-Factor Auth (MFA)	Self-Service Group Management	Self-Service Password Reset in AD	Intune MDM & MAM	Microsoft Endpoint Config Manager
Shared Account Password Roll-Over	Single-Sign-On to other SaaS	Terms of Use	3rd Party MFA Integration	System Center Endpoint Protection	Windows Server CAL Rights

Azure AD Premium Plan 2

EMS Enterprise E5 | M365 Maps

2022

THANK YOU!

Questions?