Running Your Organization Remotely - Securing Office 365 and Teams

Tuesday March 24, 2020

Peter Carson

- President, Extranet User Manager
- Office Apps and Services Microsoft MVP
- peter.carson@extranetusermanager.com
- blog.petercarson.ca
- www.extranetusermanager.com
- Twitter @carsonpeter
- President Toronto SharePoint User Group

Agenda

- Introductions
- Microsoft IT Perspectives
- Best Practices
- Multi-Factor Authentication
- Passwords
- Microsoft Services
- Summary, Q&A and Closing

RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: IDY2-F03

Breaking Password Dependencies: Challenges in the Final Mile at Microsoft

Alex Weinert (@alex_t_weinert), Director of Identity Security, Microsoft
Lee Walker, Principal Program Manager, Microsoft IT Identity and Access

https://www.rsaconference.com/usa/agenda/breaking-password-dependencies-challenges-in-the-final-mile-at-microsoft

#RSAC

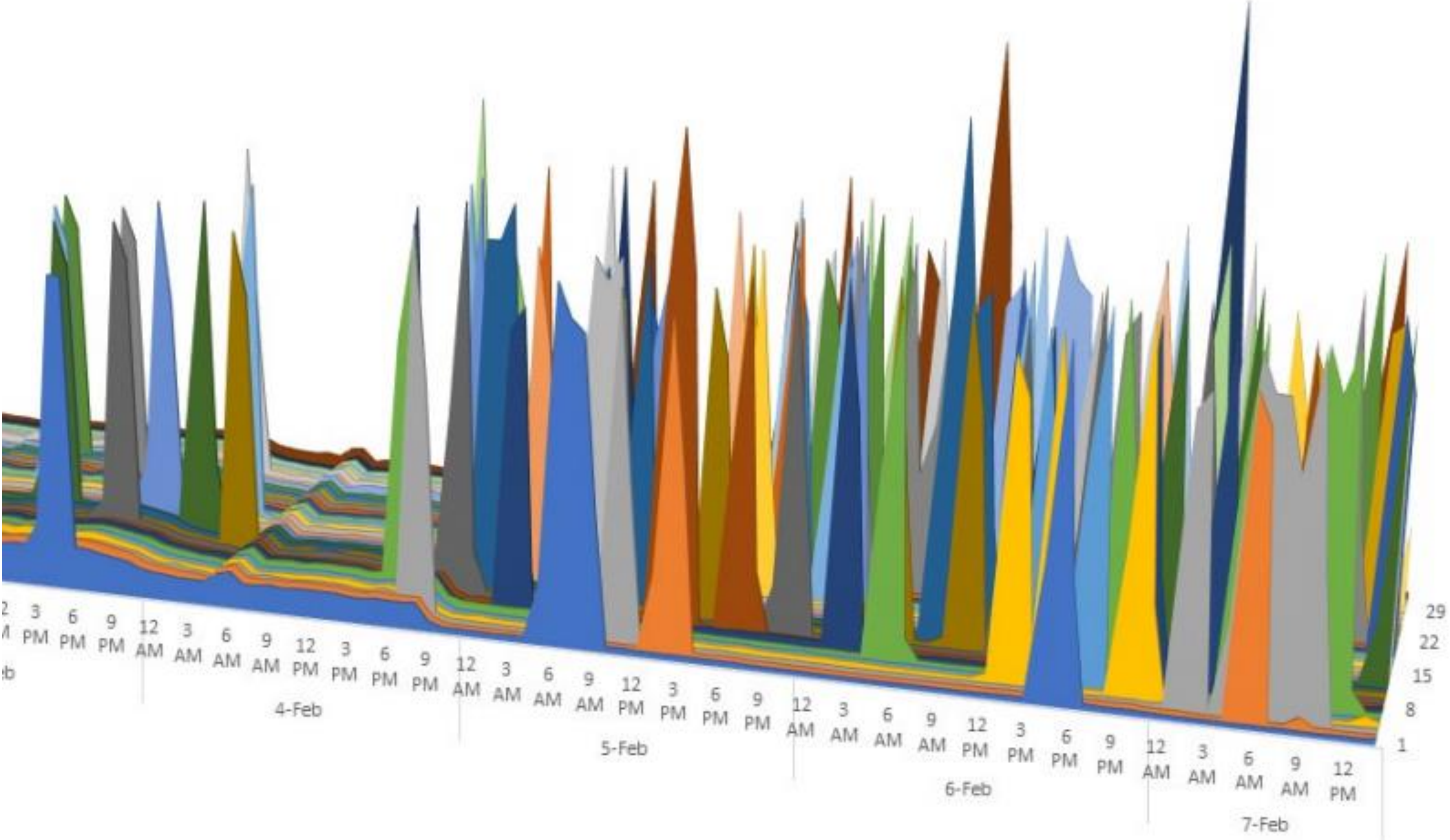
>1.2M

compromised accounts in January 2020

>99.9%

compromised accounts did not have MFA

~40% (480k accounts in January) compromised by Password Spray*



Josi@contoso.com	Spring2020!
Chance@wingtiptoys.com	Spring2020!
Rami@fabrikam.com	Spring2020!
TomH@cohowinery.com	Spring2020!
AnitaM@cohovineyard.com	Spring2020!
EitokuK@cpandl.com	Spring2020!
Ramanujan@Adatum.com	Spring2020!
Maria@Treyresearch.net	Spring2020!
LC@adverture-works.com	Spring2020!
EW@alpineskihouse.com	Spring2020!
info@blueyonderairlines.com	Spring2020!
AiliS@fourthcoffee.com	Spring2020!
[illegible]M39@litwareinc.com	Spring2020!
Margie@margiestravel.com	Spring2020!
Ling-Pi997@proseware.com	Spring2020!
PabloP@fineartschool.net	Spring2020!
GiseleD@tailspintoys.com	Spring2020!
Luly@worldwideimporters.com	Spring2020!

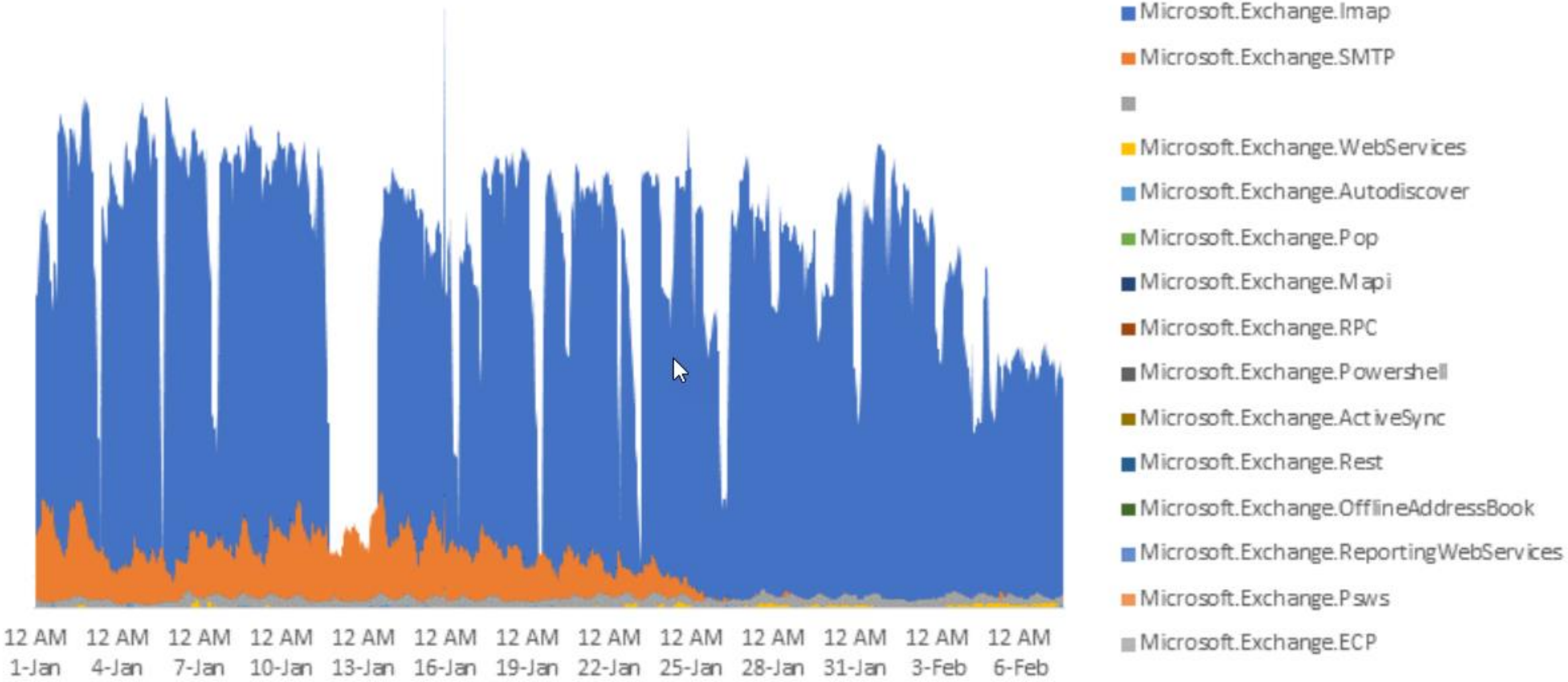
Microsoft

*Cloud detected only

>99%

of Password Spray attacks use legacy auth

~40% (480k accounts in January) compromised by replay



>97%

of Replay attacks use legacy auth

67%

Reduction in compromises in tenants who disable legacy auth

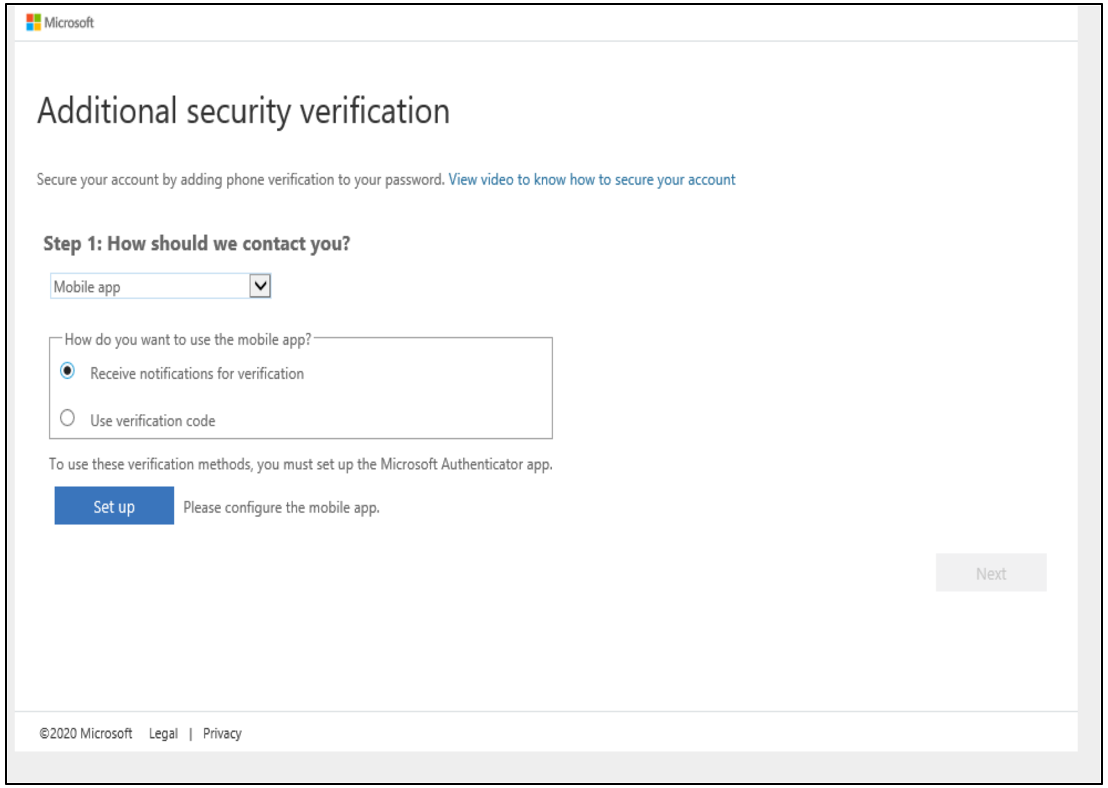
Office 365 Security Best Practices

1. Set up multi-factor authentication
2. Train your users (Educate)
3. Use dedicated admin accounts
4. Raise the level of protection against malware in mail
5. Protect Against Ransomware
6. Stop auto-forwarding for email
7. Use Office Message Encryption
8. Protect your email from phishing attacks
9. Protect against malicious attachments and files with ATP Safe Attachments
10. Protect against phishing attacks with ATP Safe Links

https://docs.microsoft.com/en-us/office365/admin/security-and-compliance/secure-your-business-data?view=o365-worldwide

Multi-Factor Authentication Setup

1. Visit https://aka.ms/MFASetup on your desktop or laptop computer
2. Go through the Microsoft login with your account
3. Select Set up for the mobile app



Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?

● Receive notifications for verification

○ Use verification code

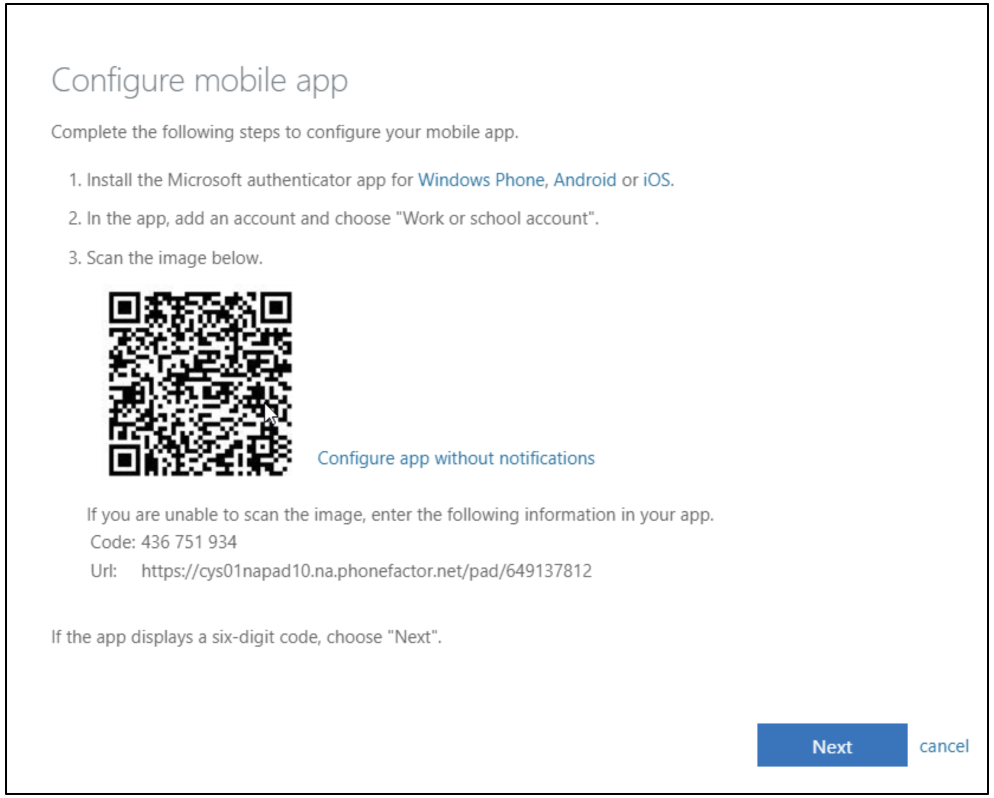
To use these verification methods, you must set up the Microsoft Authenticator app.

Please configure the mobile app.

©2020 Microsoft Legal | Privacy

Multi-Factor Authentication Setup

4. Install the iOS or Android Microsoft Authenticator app from the App Store
5. Scan the image
6. Follow the instructions on the app
7. Complete the second verification step



Configure mobile app

Complete the following steps to configure your mobile app.

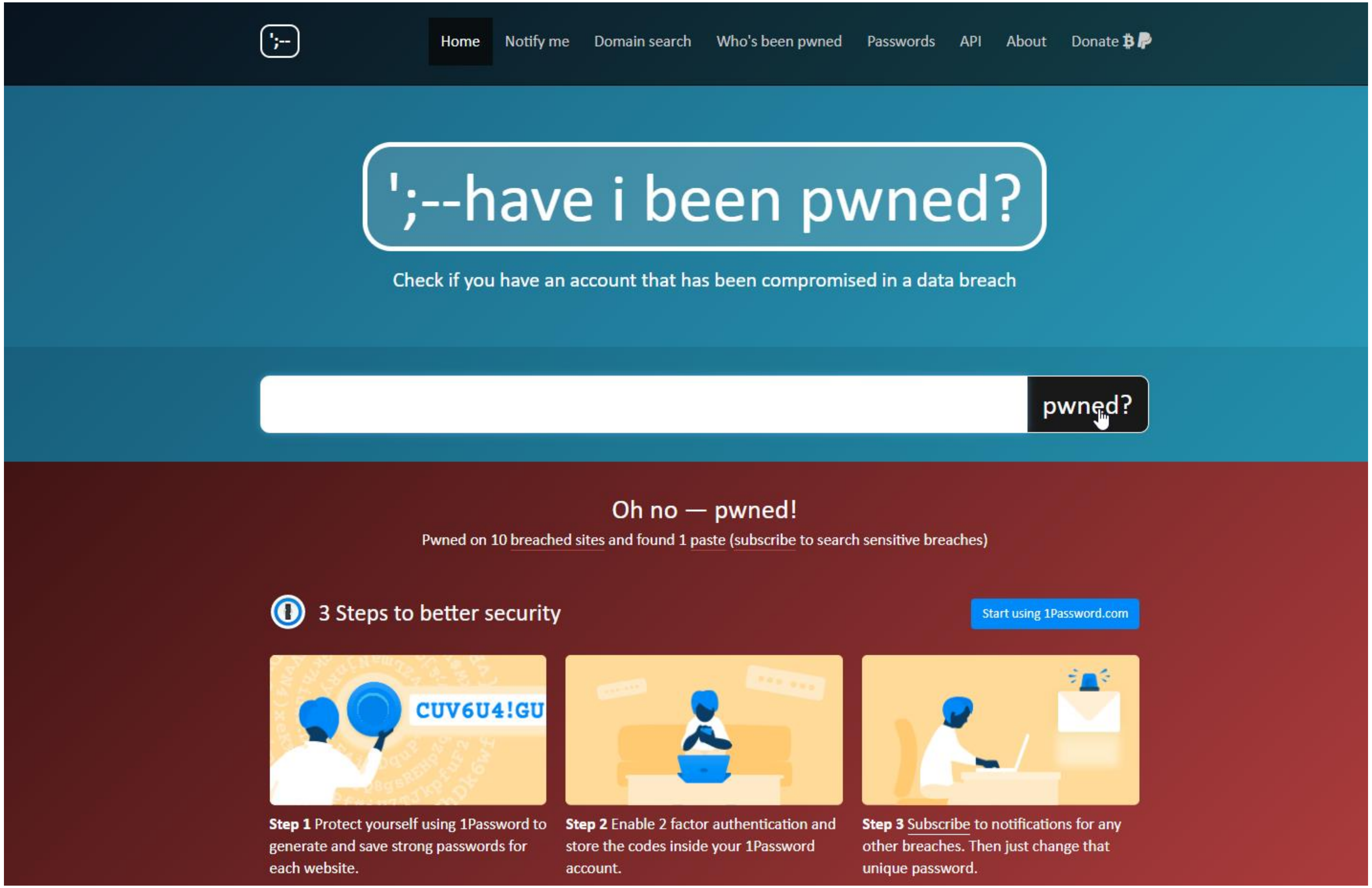
1. Install the Microsoft authenticator app for Windows Phone, Android or iOS.
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.

Configure app without notifications

If you are unable to scan the image, enter the following information in your app.
Code: 436 751 934
Url: https://cys01napad10.na.phonefactor.net/pad/649137812

If the app displays a six-digit code, choose "Next".

Passwords



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Oh no — pwned!

Pwned on 10 breached sites and found 1 paste (subscribe to search sensitive breaches)

3 Steps to better security

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

https://haveibeenpwned.com/

Have I been pwned results

- No hits
- 1 breach
- 2-9 breaches
- 10+ breaches

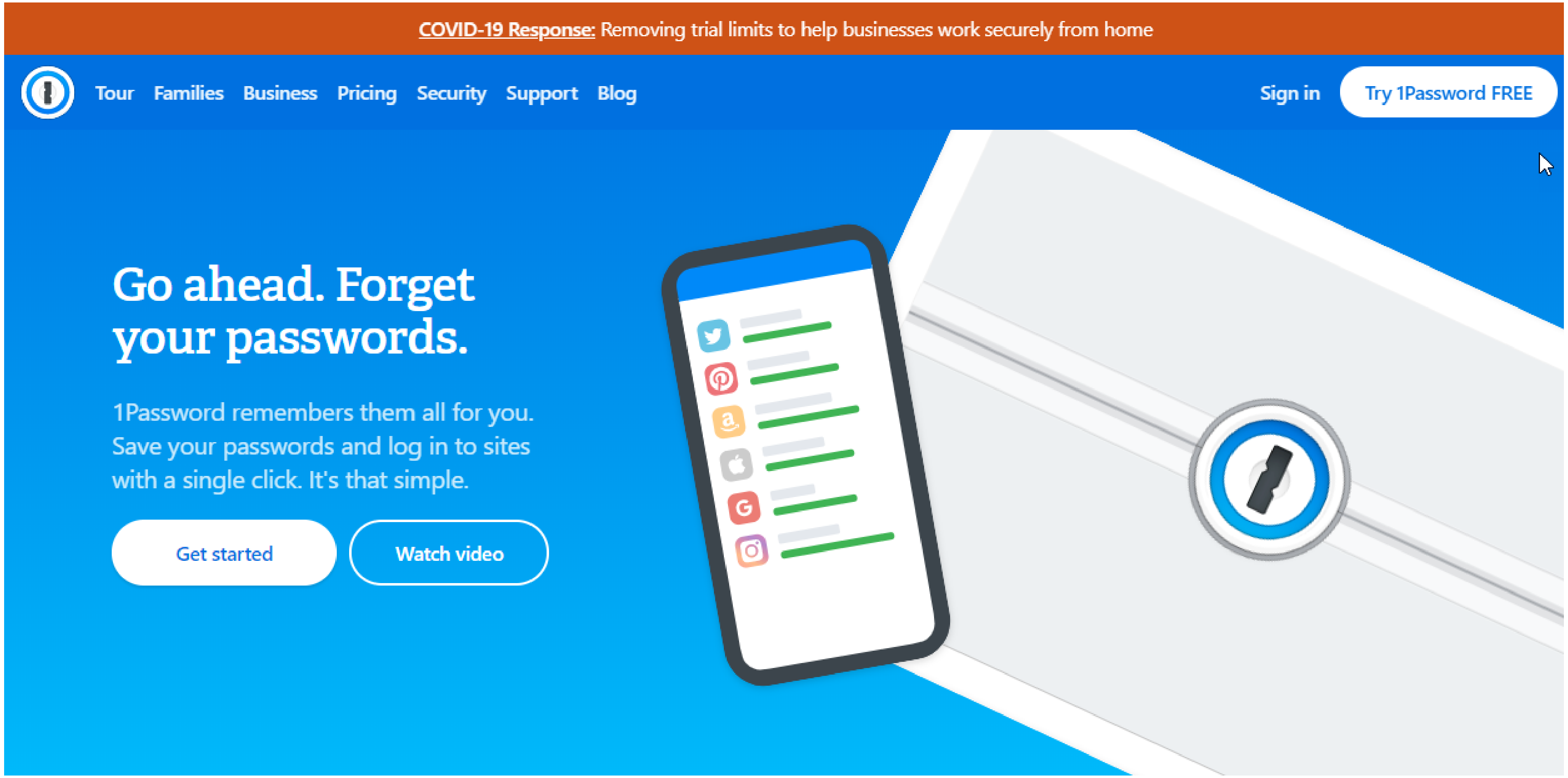
https://haveibeenpwned.com/

Password Policies

- NIST updated their guidance June 2017
- At least 8 characters in length, up to at least 64
- No complexity requirements
- No periodic password changes required
- No security questions or hints (e.g., “What was the name of your first pet?”)
- Check for compromised passwords
- Provide a password strength meter

https://en.wikipedia.org/wiki/Password_policy

https://pages.nist.gov/800-63-3/sp800-63b.html



COVID-19 Response: Removing trial limits to help businesses work securely from home

Go ahead. Forget your passwords.

1Password remembers them all for you. Save your passwords and log in to sites with a single click. It's that simple.

COVID-19 Response

6 month full featured trial

https://1password.com/

Microsoft IT’s Protection Plan

1

Passwords are weak

Continue to require MFA for modern authentication.

2

Close the backdoor

Apps not capable of MFA will be blocked.

3

Fix compromised accounts

Detect compromised accounts with Azure Identity Protection. Policy forces password change on risky users.

Licensing MFA

- **All Office 365 subscriptions include basic MFA**
  - No conditional access policies
  - Whitelisting of certain locations (such as inside the office network) can bypass MFA
    - Ensure guest WiFi is on a separate Internet IP address
- **Azure AD P1 and P2 include Conditional Access Policies**
  - Different policies can be applied
    - Include or exclude users groups, roles
    - Apps
    - Locations
    - Device Policies
    - Security Policies
  - Important to setup an Emergency account that bypasses these
    - Used if you lock yourself out
    - Password can be split across multiple people
    - Setup login alerts, this account should normally never be used

Azure AD P1 vs. P2

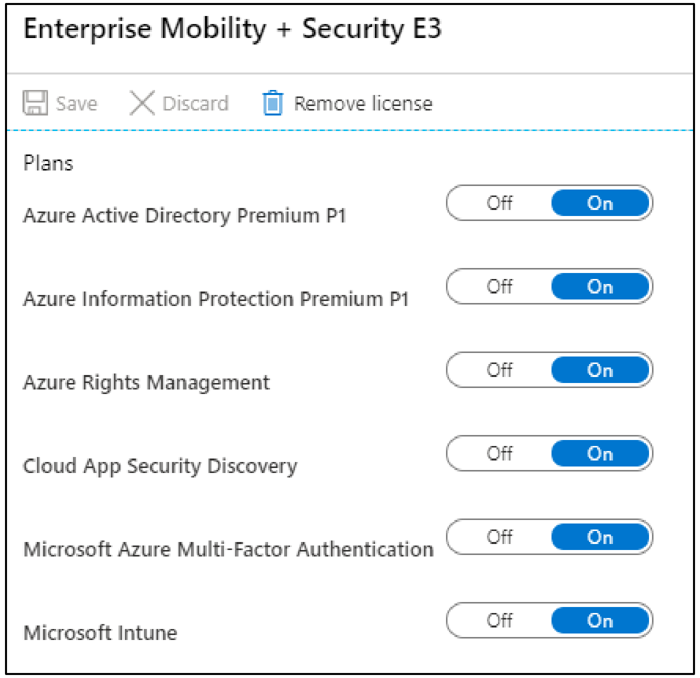
Azure AD Premium P1

- Multi-factor authentication with Conditional Access
- Hybrid Identities
- Password protection (custom banned passwords)
- Advanced Security and Usage Reports
- Conditional Access based on group, location, and device status
- AIP integration
- And Much More

Azure AD Premium P2

- Everything offered in P1
- Identity Protection
- Privileged Identity Management
- Access reviews
- Entitlement Management (Preview)

EMS E3 and E5

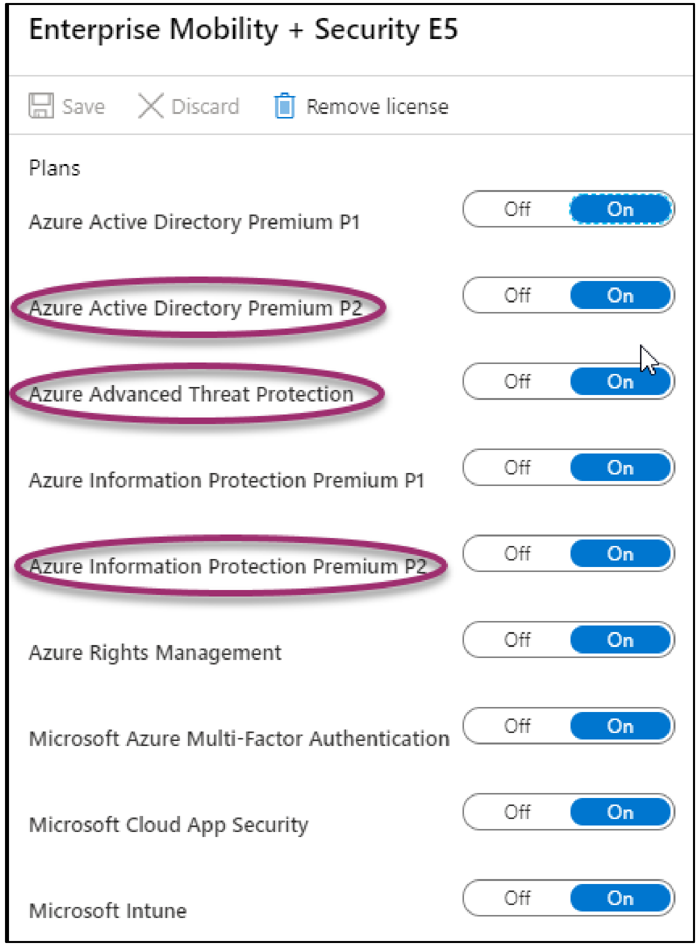


Enterprise Mobility + Security E3

Save | Discard | Remove license

Plans

Azure Active Directory Premium P1	Off [✓ On]
Azure Information Protection Premium P1	Off [✓ On]
Azure Rights Management	Off [✓ On]
Cloud App Security Discovery	Off [✓ On]
Microsoft Azure Multi-Factor Authentication	Off [✓ On]
Microsoft Intune	Off [✓ On]



Enterprise Mobility + Security E5

Save | Discard | Remove license

Plans

Azure Active Directory Premium P1	Off [✓ On]
Azure Active Directory Premium P2	Off [✓ On]
Azure Advanced Threat Protection	Off [✓ On]
Azure Information Protection Premium P1	Off [✓ On]
Azure Information Protection Premium P2	Off [✓ On]
Azure Rights Management	Off [✓ On]
Microsoft Azure Multi-Factor Authentication	Off [✓ On]
Microsoft Cloud App Security	Off [✓ On]
Microsoft Intune	Off [✓ On]

Microsoft 365

Office 365

Windows 10

Microsoft 365 E3

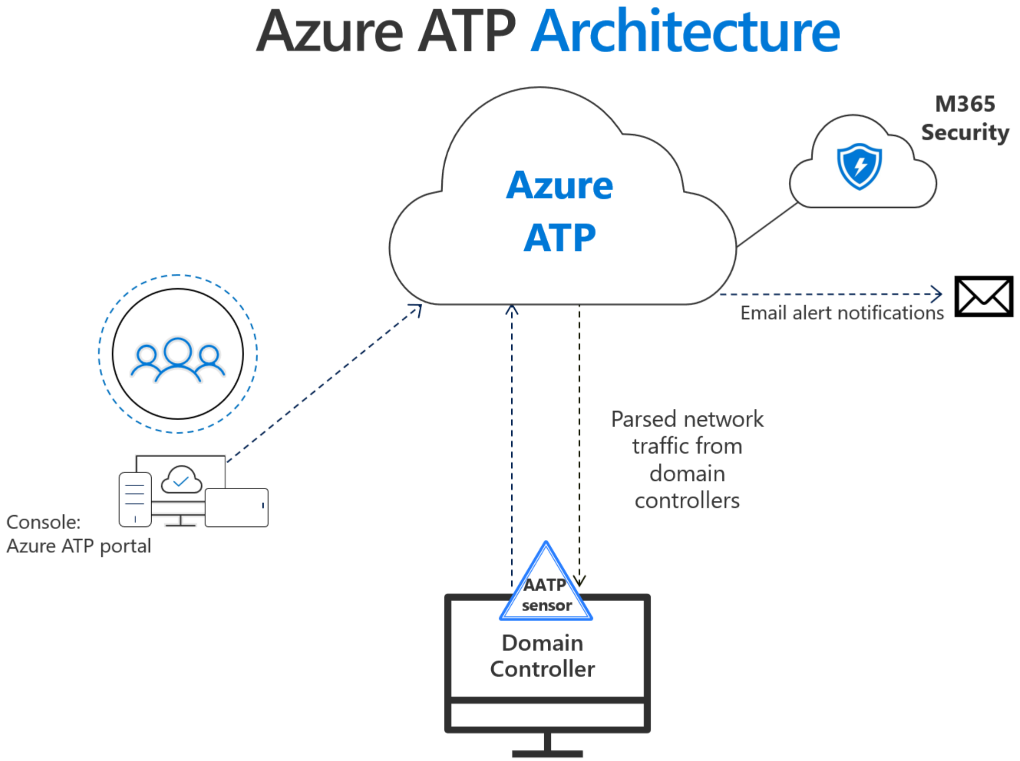
- Office 365 E3
- EMS E3
- Windows 10

Microsoft 365 E5

- Office 365 E5
- EMS E5
- Windows 10

Azure Advanced Threat Protection (ATP)

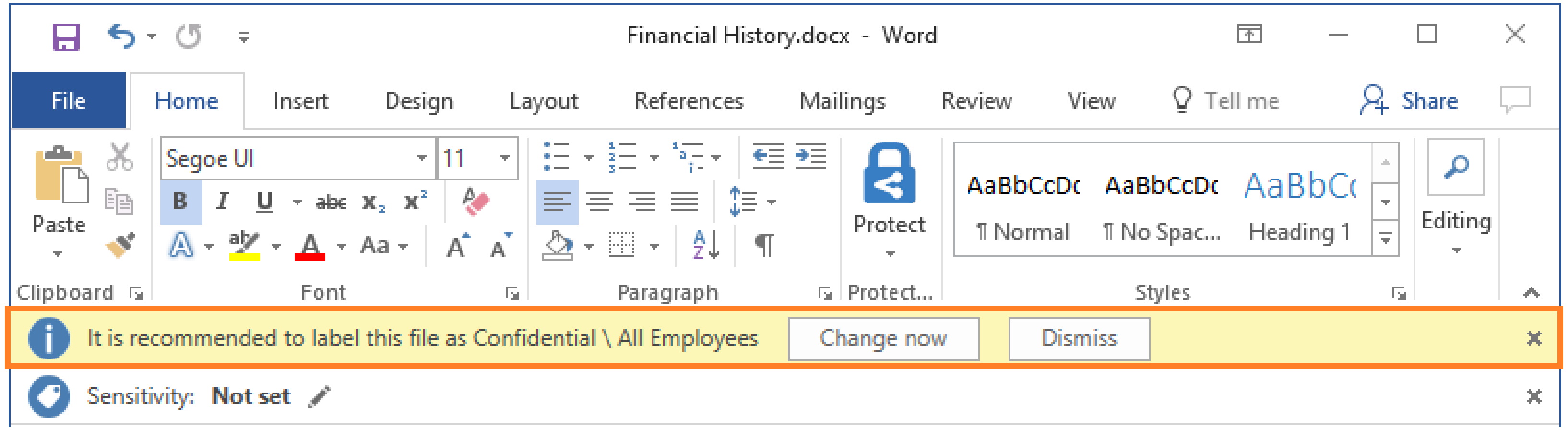
- Cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
- Monitor users, entity behavior, and activities with learning-based analytics
- Protect user identities and credentials stored in Active Directory
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
- Provide clear incident information on a simple timeline for fast triage


Azure ATP Architecture
Azure ATP
M365 Security
Email alert notifications
Parsed network traffic from domain controllers
Console: Azure ATP portal
AATP sensor
Domain Controller

https://docs.microsoft.com/en-us/azure-advanced-threat-protection/what-is-atp

Azure Information Protection (AIP)

- Cloud-based solution that helps an organization to classify and protect its documents and emails by applying labels
- Labels can be applied automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations
- Uses Azure Rights Management - protection that is applied by using Rights Management stays with the documents and emails, independently of the location—inside or outside your organization, networks, file servers, and applications.



It is recommended to label this file as Confidential \ All Employees

Sensitivity: **Not set**

https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

Layering Up Your Security Implementation

1. **MFA is the most important feature you can turn on**
   - Office 365 provides basic MFA which prompts on every login
   - Conditional access lets you define rules for MFA
     - Managed versus unmanaged device
     - Risk level
     - Locations
     - Apps
2. **Azure Information Protection can classify content**
   - Can be used with Conditional Access to determine policy
   - Can be manually or automatically applied
3. **Advanced Threat Protection can help secure your on-premise environment**

Microsoft Security Licensing Options

- **Purchase as part of a bundle**
  - Microsoft 365 E3 or E5
    - Superset of Office 365 E3 or E5
  - Enterprise Mobility + Security E3 or E5
    - Bundled into Microsoft 365

- **Individual step up plans**
  - Azure AD Premium P1 or P2
  - Azure Advanced Threat Protection
  - Azure Information Protection P1 or P2
  - Azure Rights Management
  - Cloud App Security
  - Intune

Office 365 MFA is included in all Office 365 subscriptions

Upcoming Events

Extranet User Manager Webinar
Extending Office 365 and Teams to your Partners
March 25, 2020
12 pm – 12:30 pm EST

Eum.co/events

Extranet User Manager Webinar
Forms and Flow Employee Self-Service (Part 1 of 2)
April 7, 2020
12 pm – 12:30 pm EST

Eum.co/events

Thank you!

Questions?