Microsoft

Microsoft Ignite

Learn.
Connect.
Explore.

Microsoft

BRK3251

Shut the door to cybercrime with identity-driven security

Nitika Gupta (@_Nitika_Gupta)
Mark Morowczynski (@markmorow)
Program managers
Identity

About a year ago….

- Top 3 Identity attacks
  - Password Spray
  - Phishing
  - Breach Replay

Microsoft Ignite 2017

Shut the door to cybercrime with Azure Active Directory risk-based identity protection

Oct 11, 2017 at 12:45PM by Nitika Gupta, Alexander Weinert

★★★★★ 0 ratings

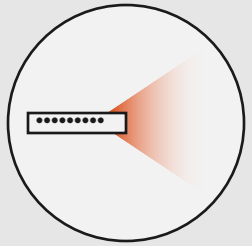
I heard about this new advanced attack...

Consent Abuse

IoT

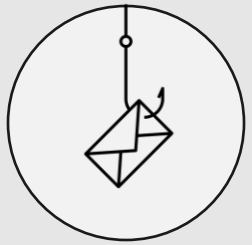
Nation State

Current Attacks and What YOU NEED to Do About It



Password Spray

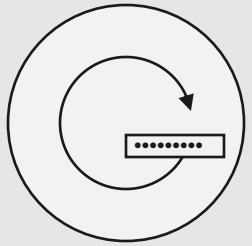
200,000 accounts compromised in Aug 2018



Phishing

5B emails blocked in 2018

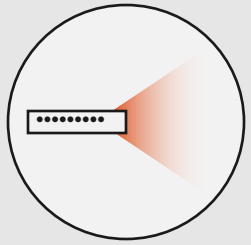
44M risk events in Aug 2018



Breach replay

650,000 accounts with leaked credentials in 2018

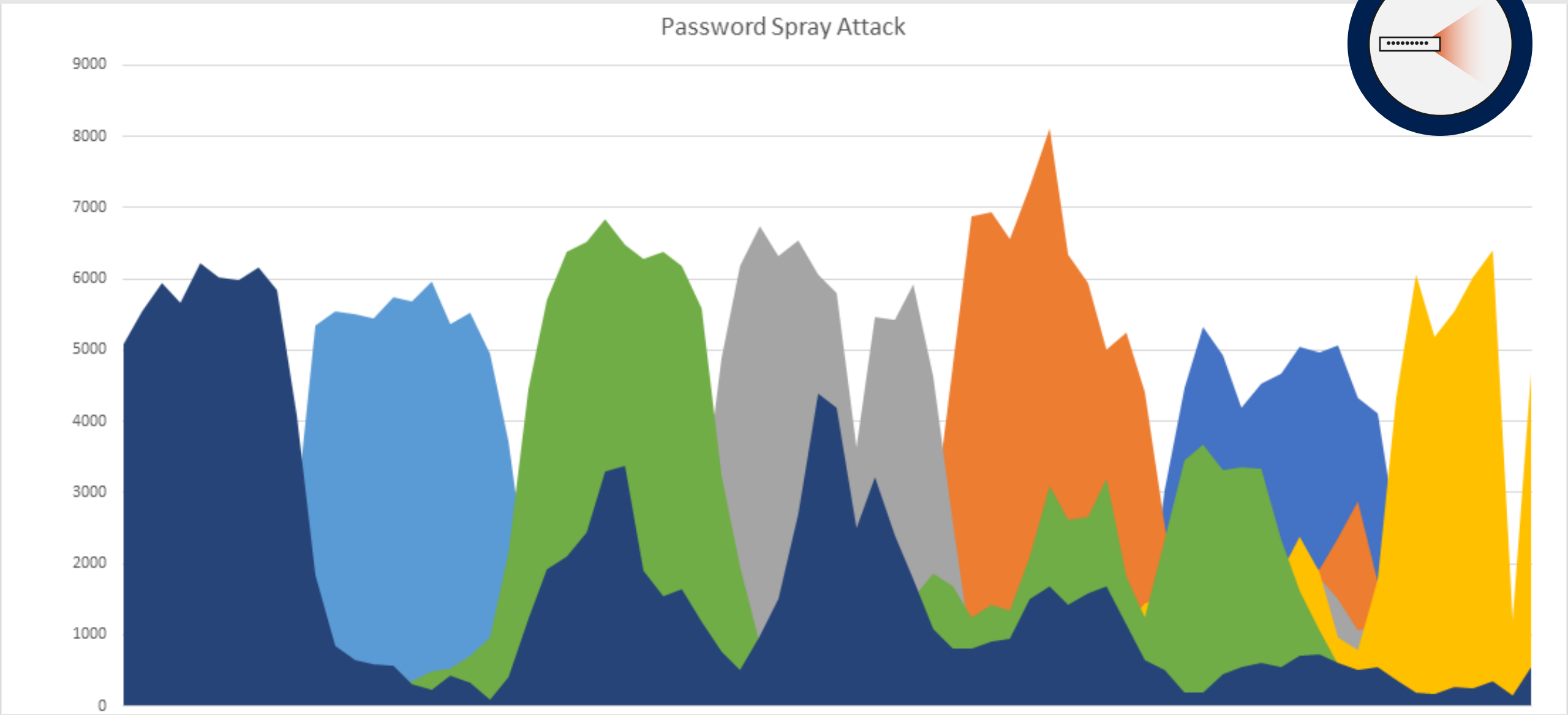
Bonus: App Consent



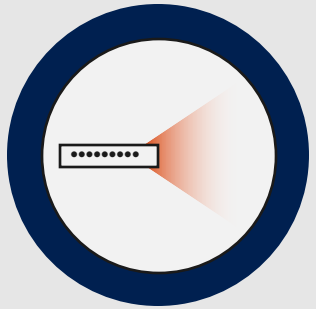
Password Spray

- 1 Common password used against many, many accounts.
- Below account lockout threshold
- After successful login, dump the GAL.
- Start pivoting in environment.

Josi@contoso.com	Ignite2018
Chance@wingtiptoys.com	Ignite2018
Rami@fabrikam.com	Ignite2018
TomH@cohowinery.com	Ignite2018
AnitaM@cohovineyard.com	Ignite2018
EitokuK@cpandl.com	Ignite2018
Ramanujan@Adatum.com	Ignite2018
Maria@Treyresearch.net	Ignite2018
LC@adverture-works.com	Ignite2018
EW@alpineskihouse.com	Ignite2018
info@blueyonderairlines.com	Ignite2018
AiliS@fourthcoffee.com	Ignite2018
MM39@litwareinc.com	Ignite2018
Margie@margiestravel.com	Ignite2018
Ling-Pi997@proseware.com	Ignite2018
PabloP@fineartschool.net	Ignite2018
GiseleD@tailspintoys.com	Ignite2018
Luly@worldwideimporters.com	Ignite2018
Bjorn@woodgrovebank.com	Ignite2018
NK@lucernepublishing.com	Ignite2018

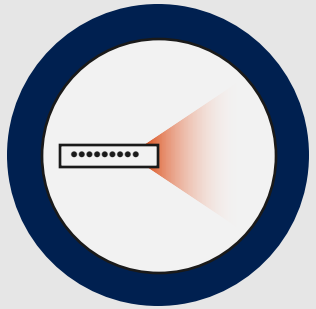

Password Spray Attack
9000
8000
7000
6000
5000
4000
3000
2000
1000
0

How common is it?



- 200,000 accounts compromised in Aug 2018
- Primarily from legacy authentication protocols that are preferred by bad actors

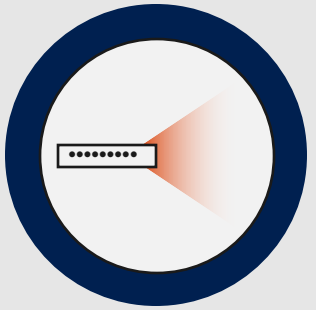
Go Do #1



- Banned password
  - Cloud only: Check
  - Hybrid:
    - Change/Reset passwords in cloud using password writeback and self service password reset
    - On-prem banned password filter
  - Policy: Update your Password Policy
    - Microsoft Password Guidance White Paper
    - NIST 800-63B
- Banned password tried in Azure AD in last 30 days
  - % of Users Attempting Banned Passwords= 15.6%

On-Prem Banned Password

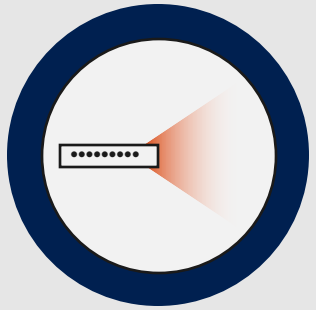
Go Do #2



- Block suspicious IPs
  - Cloud only: check
  - Hybrid:
    - Cloud authentication: Check
    - Risky IP report in Connect Health
      - ADFS
- Risky IP report usage:
  - 3K+ onboarded ADFS customers
  - 400-500 monthly active customers

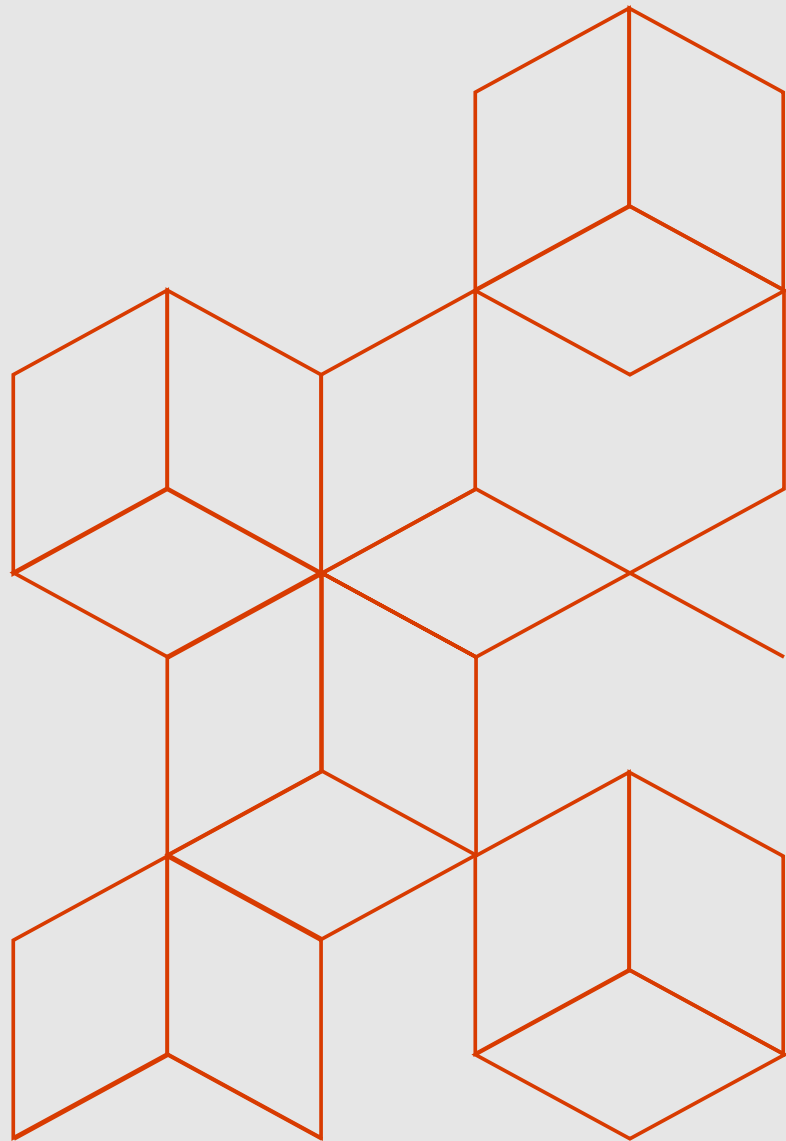
Risky IP

Go Do #3



- Block legacy auth
  - Cloud only: Azure AD Conditional access
  - Hybrid: Azure AD Conditional access
- Over 5000 tenants using block legacy auth CA policy
- Go See Best Practices from Around the World Friday

Blocking Legacy Auth



Phishing

Evolving Threat Landscape | Phish by Numbers

12B

BEC attributed loss since 2013

5B

Phish mails blocked in Office 365 in 2018

300K

Phish Campaigns analyzed in 2018

1B

Mails with malicious links seen in 2018

20% in 5 Minutes

Clicks in first 5 mins

4%

Users always click on a phishing link

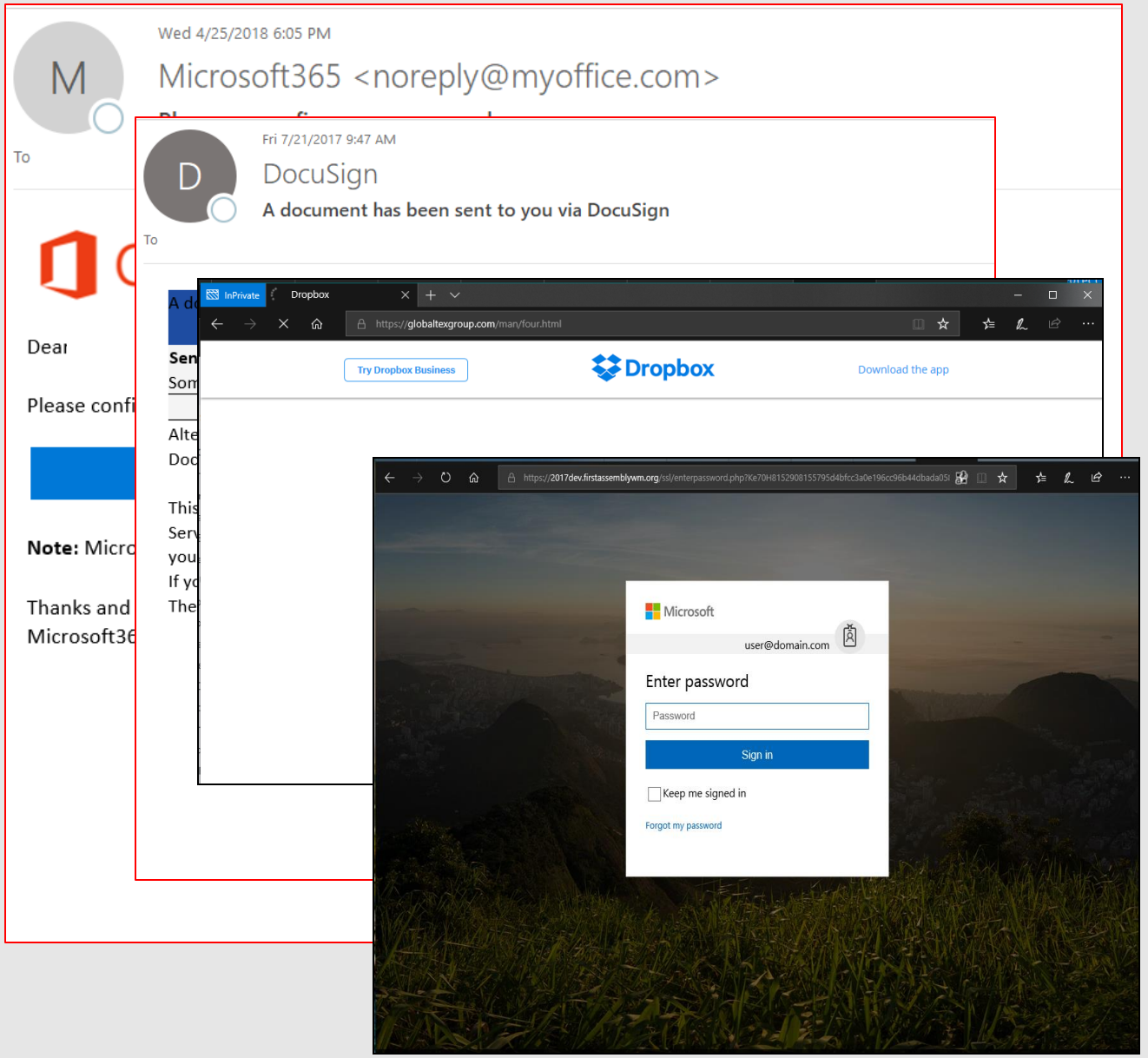
Polymorphic Parallel Attacks | Short Span Attacks | Serial Variant Attacks | Shared Cloud/SaaS Infrastructure

Source: Microsoft, Verizon

Attack Delivery/Exploitation (1)

Credential harvesting

- Spoofed Domain
- Brand Impersonation
- Compromised Account
- Malicious Link (New domain/compromised site)
- Malicious Attachments



Recipient clicks on link and enters credentials or downloads malware

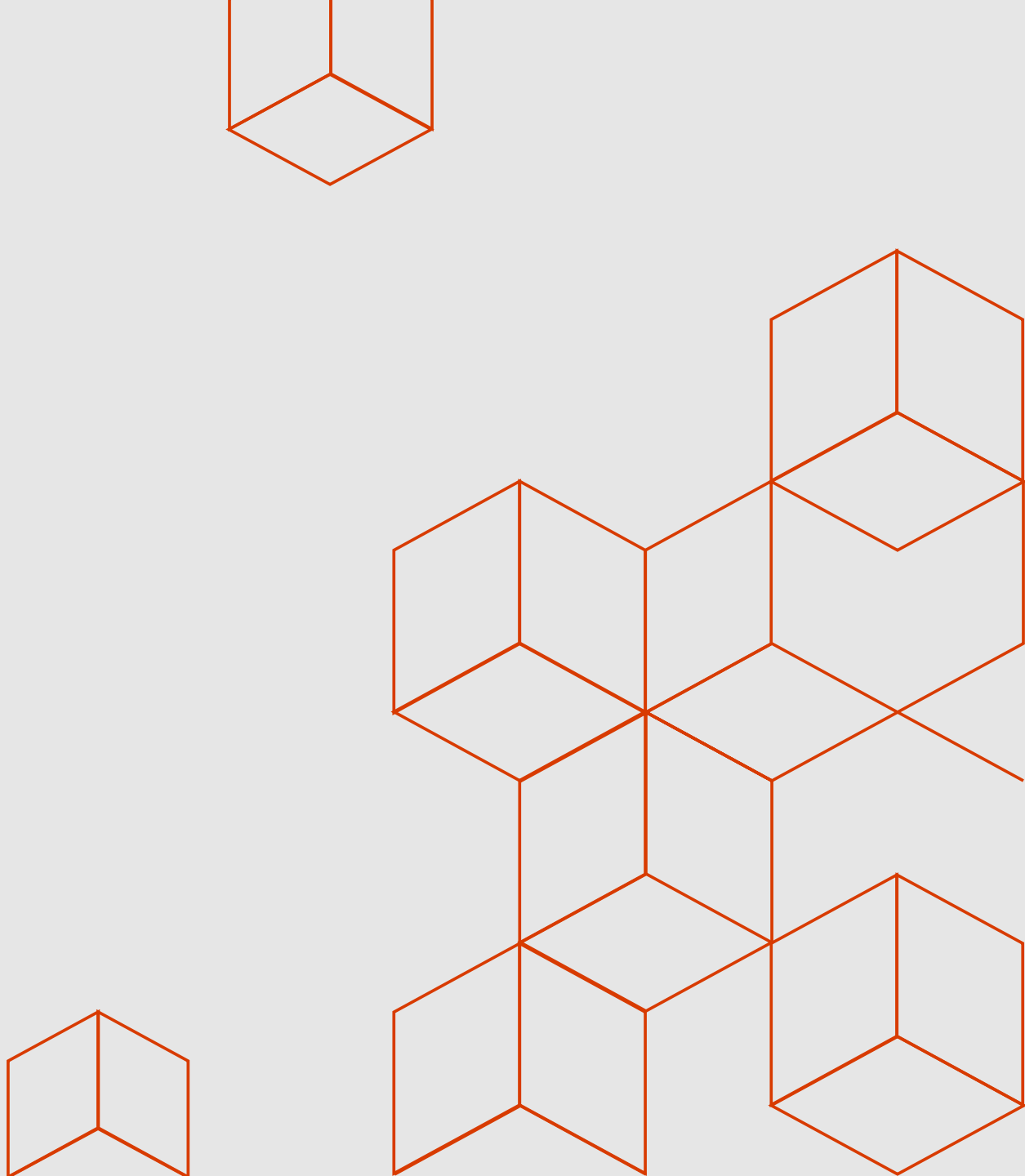
How common is it?

44M risk events in Aug 2018

Go Do #4

- Monitor your risk reports
  - Risky sign-in
  - User risk

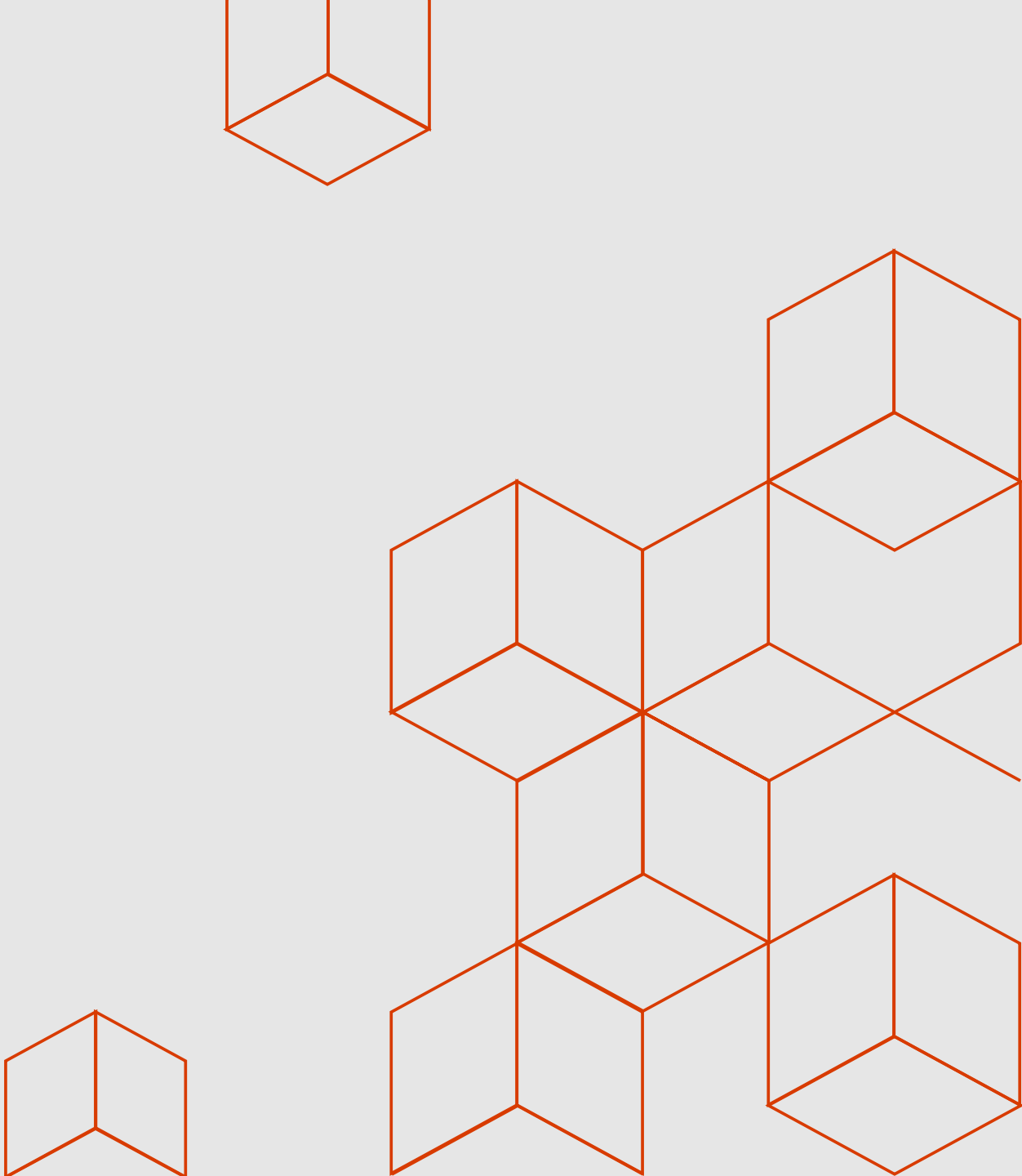
Risk Reports



Go Do #5

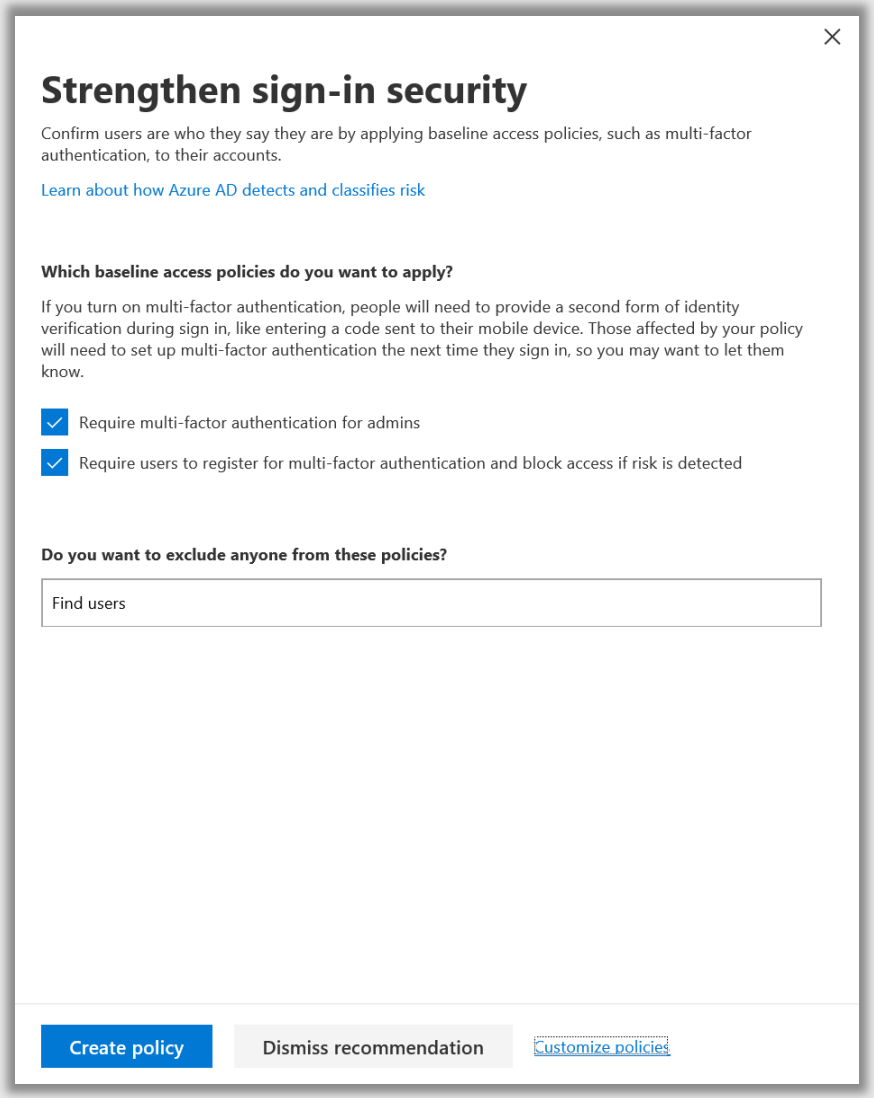
- Enable MFA for users using Conditional Access
- Enable Sign-in risk policy

Sign-in risk policy

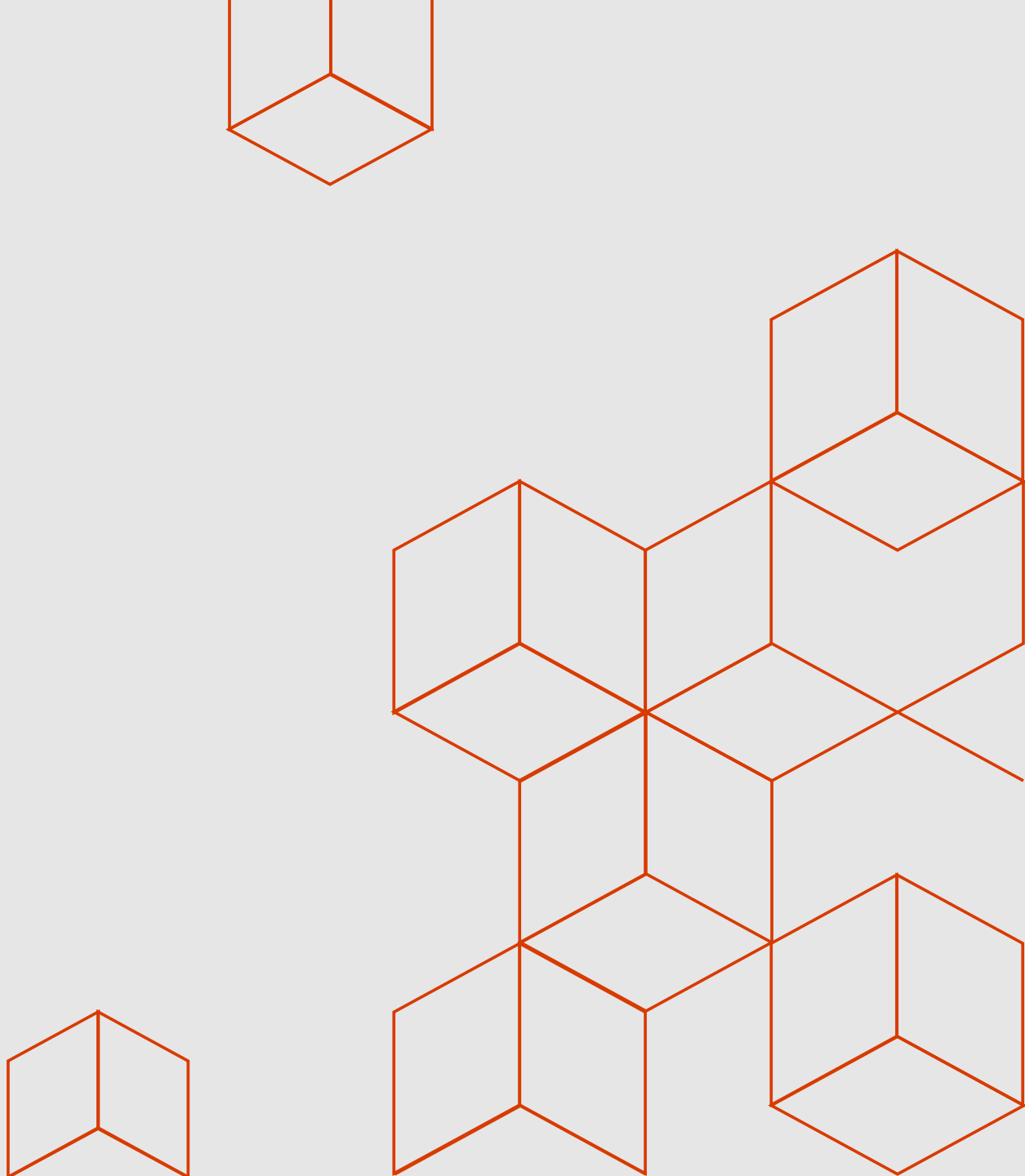


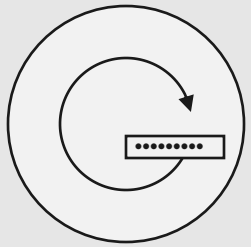
Baseline policy for end users (public preview coming soon!)

- Enroll all users in the Microsoft authenticator app for MFA
- Protect all users with the Microsoft authenticator app or block when risk is detected



Baseline Protection for end users





Breach replay

Username
TroubledTimerMoto83
Password
mxt60JhTRx45G110kLn6F
Enter>

USERNAME
TroubledTimerMoto83
PASSWORD
mxt60JhTRx45G110kLn6F
SUBMIT
Forgot your password or user name? Click Here.

Username: TroubledTimerMoto83
Password: mxt60JhTRx45G110kLn6F
Submit

What is Breach Replay

- End users use the same username and passwords on many sites
- Sometimes it is for a good reason
- Sometimes it is for a terrible reason
- Username/Password pairs are posted online, bad guys use them.

How common is it?

Credentials processed in 2018 — 2 billion

Credentials matched in 2018 — 650,000

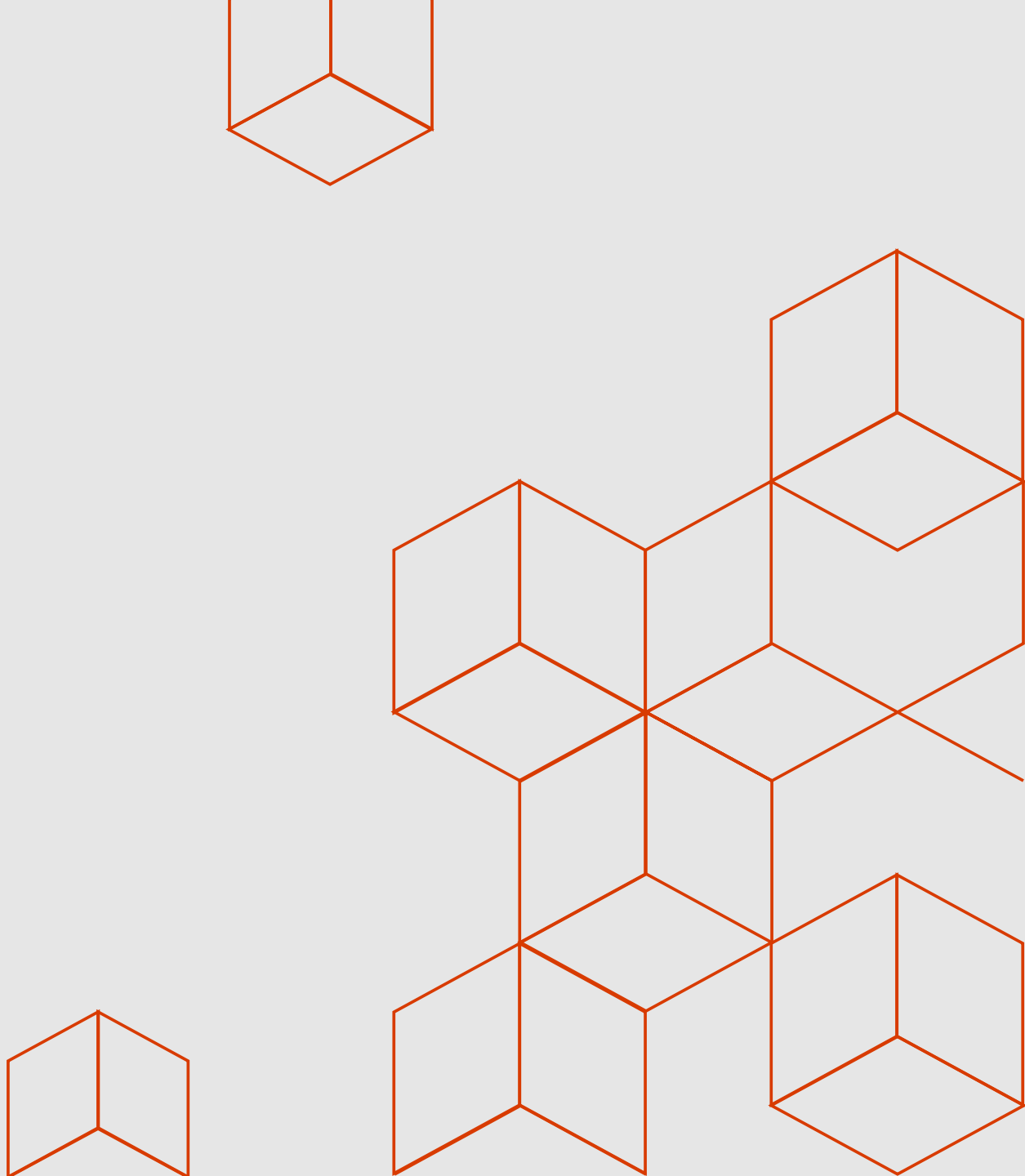
Go Do #6

- Turn on Password Hash Sync
- Enabled for 82% Azure AD active tenants
- 57% of Azure AD active users

Go Do #7

- Enable User Risk Based policy

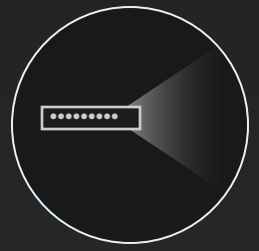
User Risk Based Policy



Current

Emerging

Password Spray

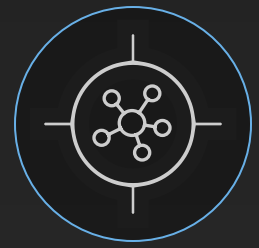


Phishing

Breach Replay

Consent abuse

IoT attacks



Nation state

A brief history of bad consent apps….

Mar 15th, 2017 – Fancy Bear employs OAuth phishing attack on US elections

- Used to maintain persistent access to data

April 25th, 2017 – Russian Hackers allegedly use OAuth in attempts to interfere with French election

- Leveraging OAuth connected apps for additional intel

May 5th, 2017 – Fake Google Docs OAuth App

- Phishing campaign to tricking users into consenting to fake extracting contacts and email addresses

Nov 6th, 2017 – OceanLotus intel gathering attack breaks news

- Targeted attack directing users to consent to app gaiting access to important documents

Jan 13th, 2018 – Kevin Mitnick, PoC OAuth cloud ransomware

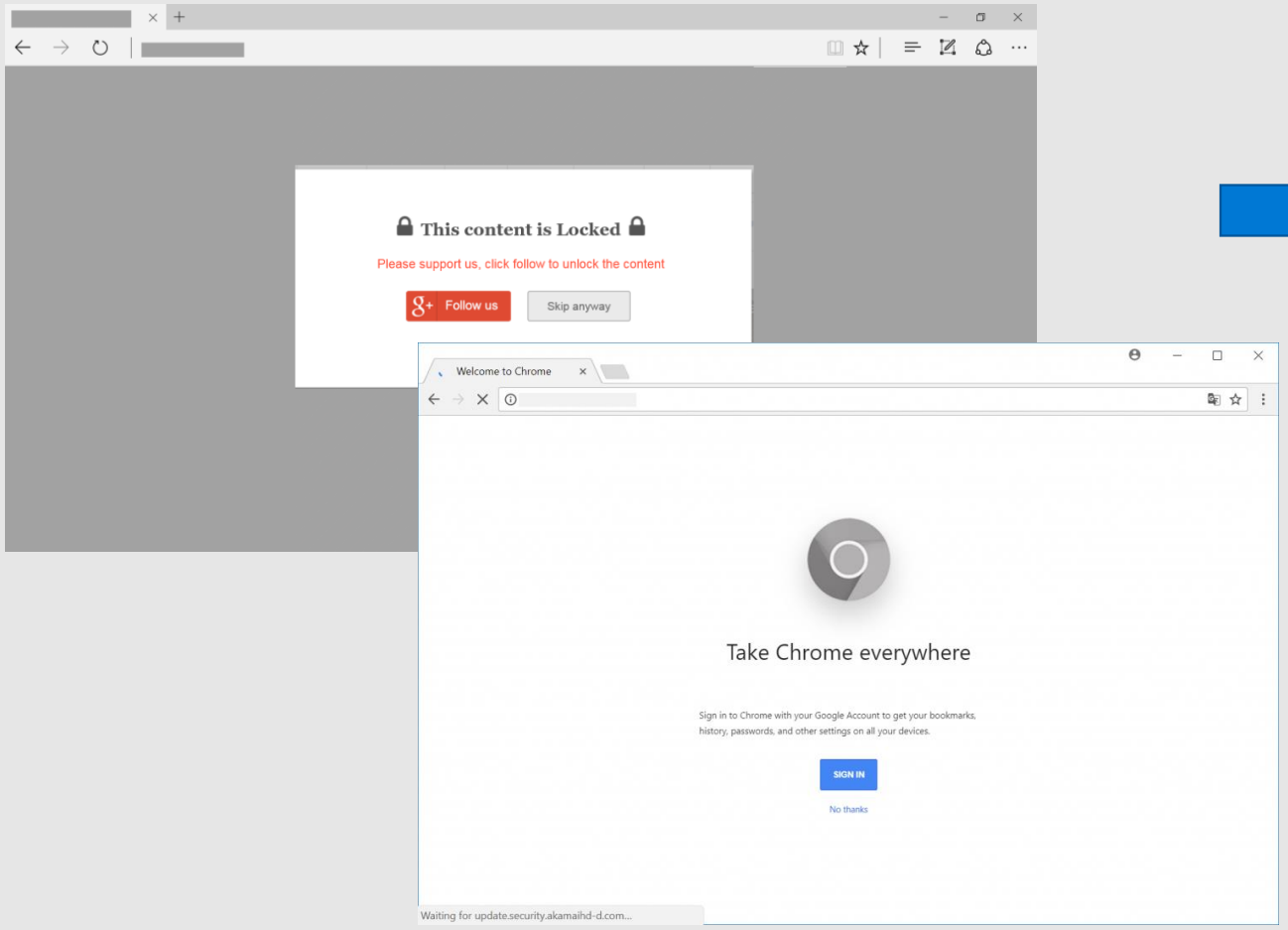
- Consent to fake app leading to email download, deletion, and encryption, requesting money to restore.

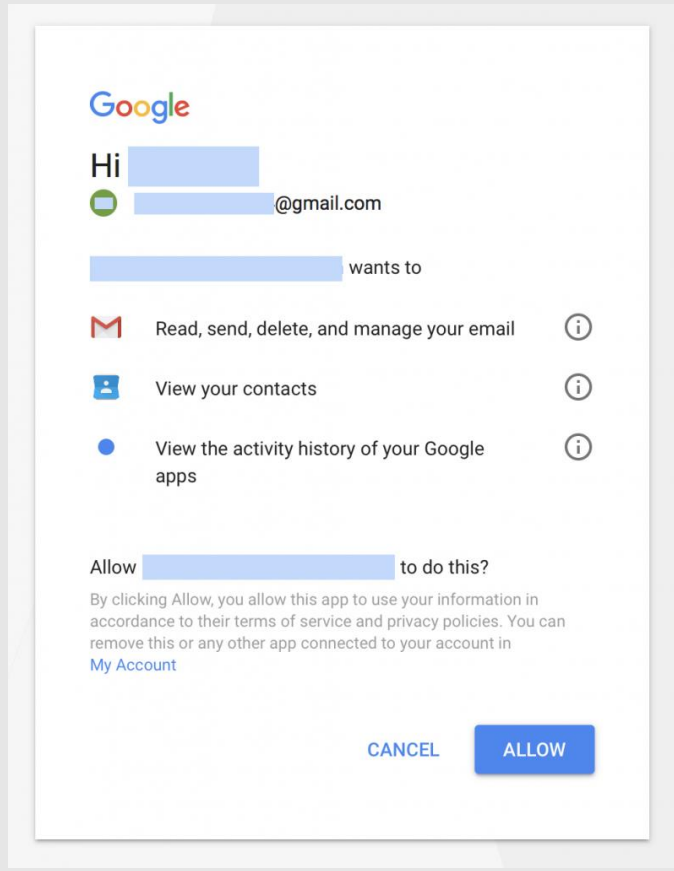
Mar, 2018- Cambridge Analytica data scandal exposed

- Seemingly good application that proliferated data misuse

OceanLotus – OAuth espionage

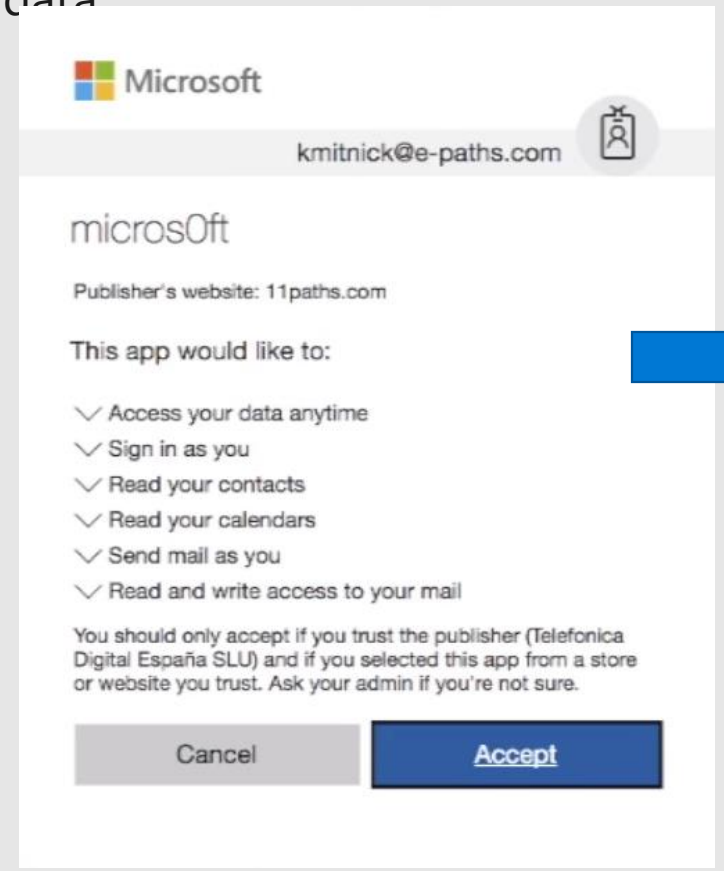
1. User tricked into navigating to compromised site.
2. Site exploit looks for specific users/accounts/characteristics and selectively displays malicious content
3. Malicious content is clicked, leading to a consent request for a malicious app.

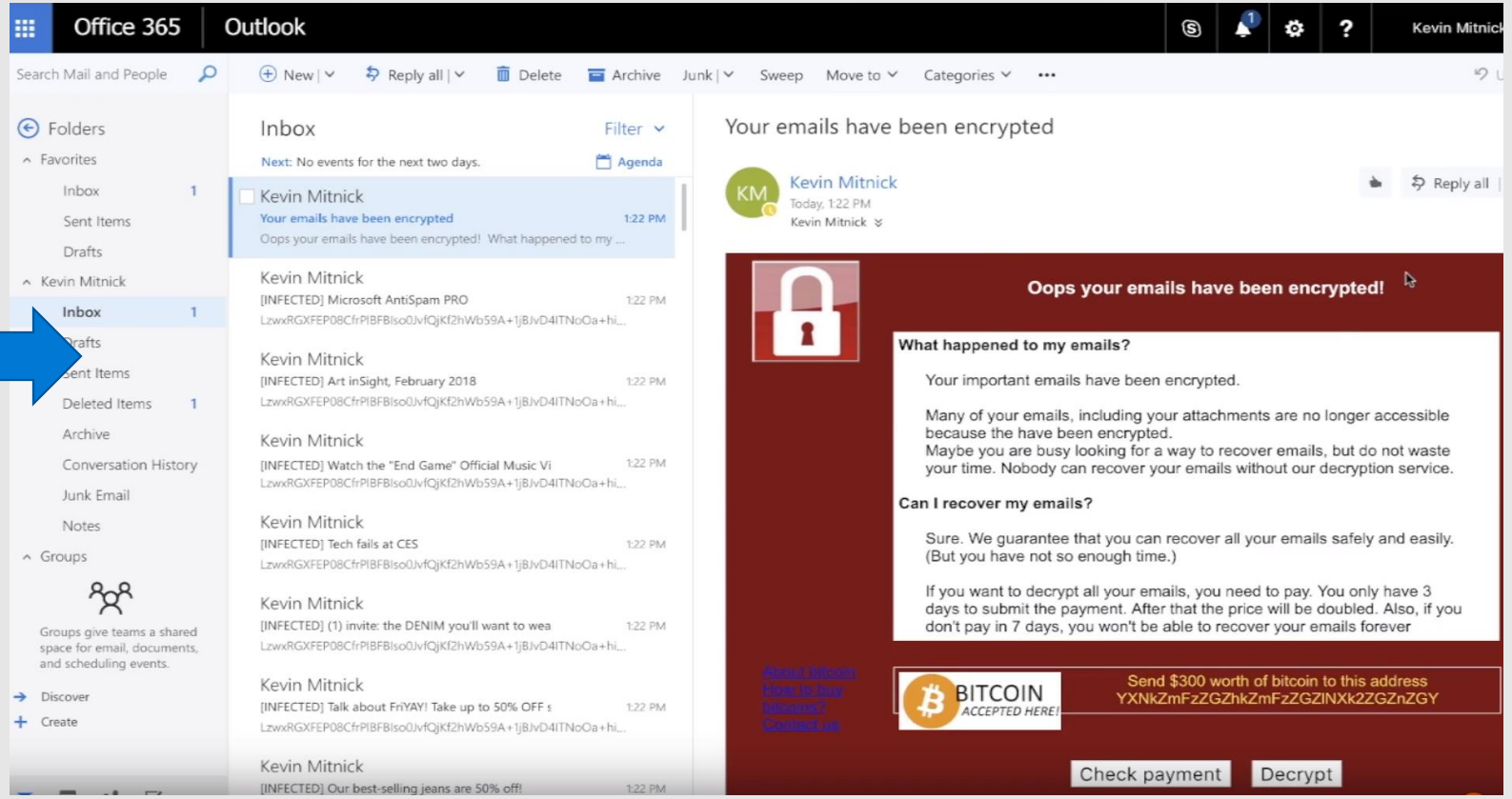




Cloud Ransomware - Malicious applications

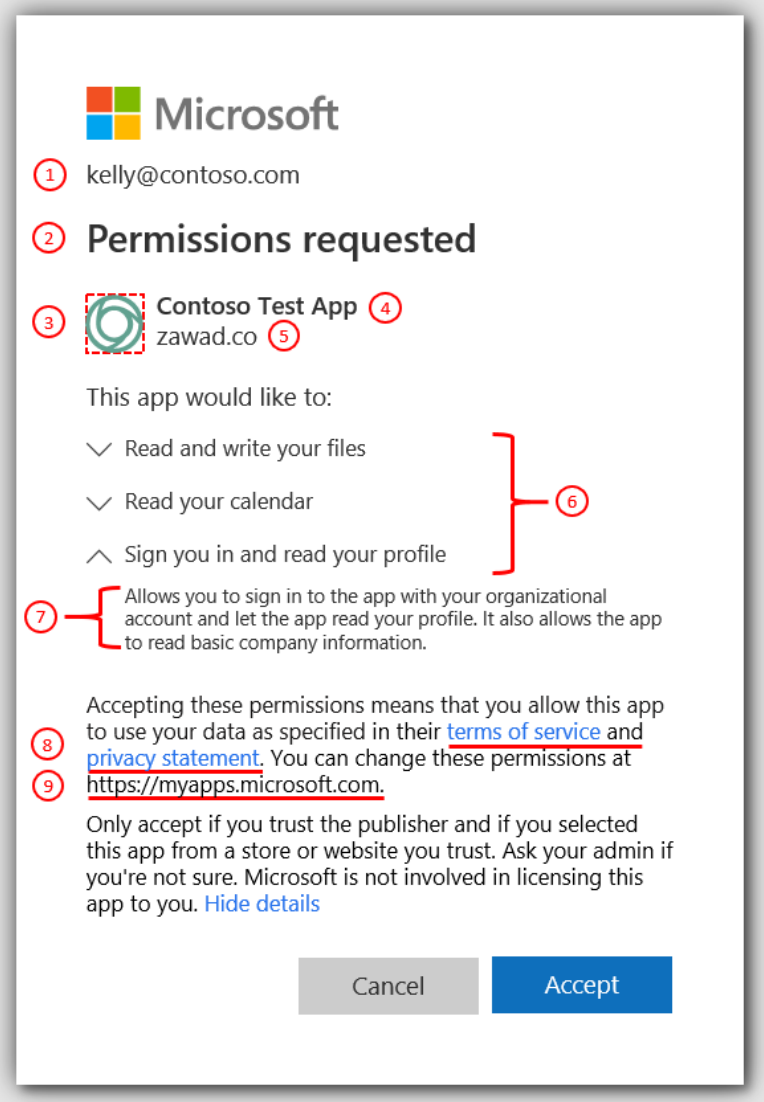
1. User grants scoped data access to app “Office 365 Mail” (PoC used “micr0soft”)
2. App takes over mailbox, downloads all mail, encrypts contents, and requests ransom to regain data





Example of a cloud ransomware attack

Reduce the risk through education

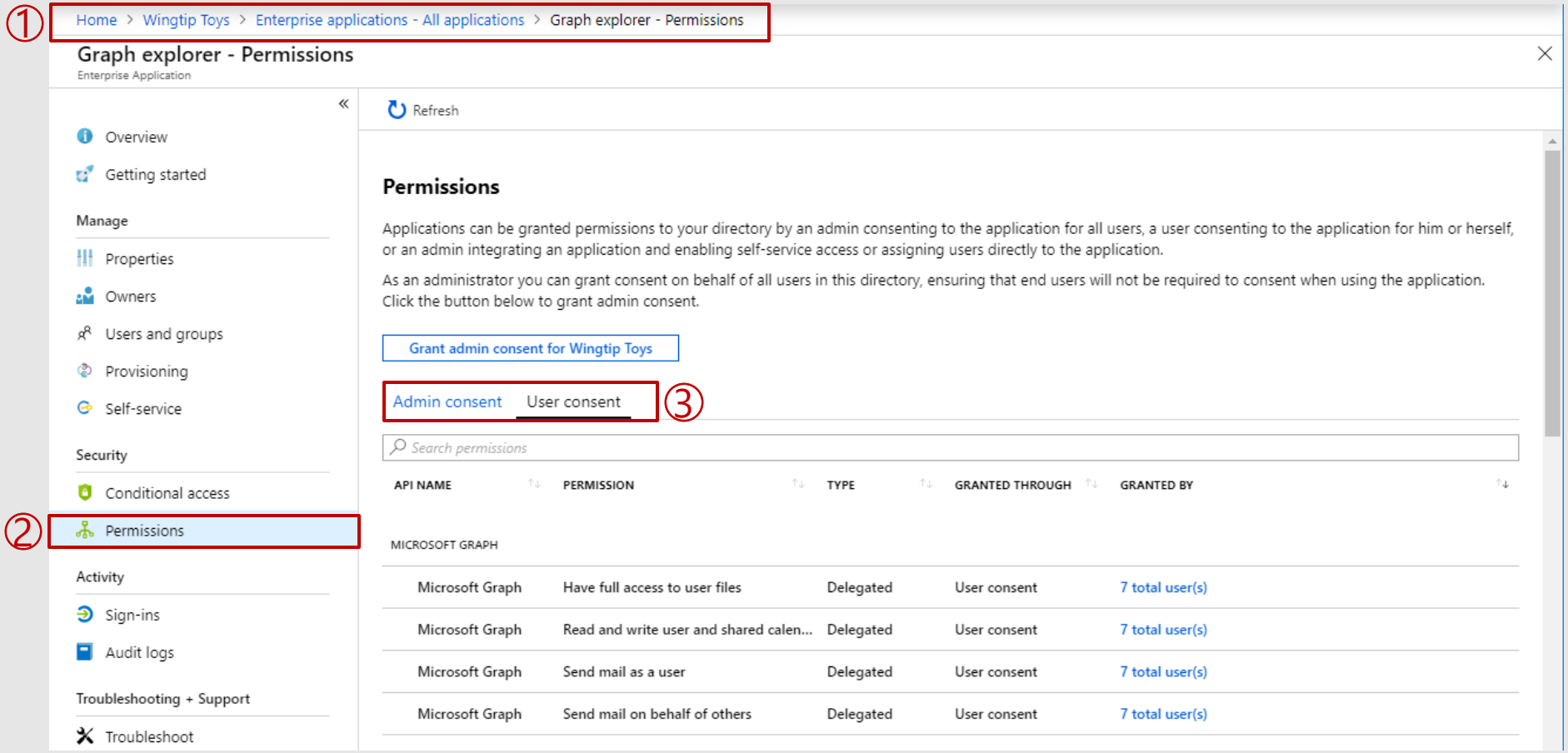


#	Component	Purpose
1	User identifier	This identifier represents the user that the client application is requesting to access protected resources on behalf of.
2	Title	The title changes based on whether the users are going through the user or admin consent flow. In user consent flow, the title will be “Permissions requested” while in the admin consent flow the title will have an additional line “Accept for your organization”.
3	App logo	This image should help users have a visual cue of whether this app is the app they intended to access. This image is provided by application developers and the ownership of this image isn't validated.
4	App name	This value should inform users which application is requesting access to their data. Note this name is provided by the developers and the ownership of this app name isn't validated.
5	Publisher domain	This value should provide users with a domain they may be able to evaluate for trustworthiness. This domain is provided by the developers and the ownership of this publisher domain is validated.
6	Permissions	This list contains the permissions being requested by the client application. Users should always evaluate the types of permissions being requested to understand what data the client application will be authorized to access on their behalf if they accept. As an application developer it is best to request access, to the permissions with the least privilege.
7	Permission description	This value is provided by the service exposing the permissions. To see the permission descriptions, you must toggle the chevron next to the permission.
8	App terms	These terms contain links to the terms of service and privacy statement of the application. The publisher is responsible for outlining their rules in their terms of service. Additionally, the publisher is responsible for disclosing the way they use and share user data in their privacy statement. If the publisher doesn't provide links to these values for multi-tenant applications, there will be a bolded warning on the consent prompt.
9	Myapps URL	This is the link where users can review and remove any non-Microsoft applications that currently have access to their data.

https://docs.microsoft.com/en-us/azure/active-directory/application-consent-experience

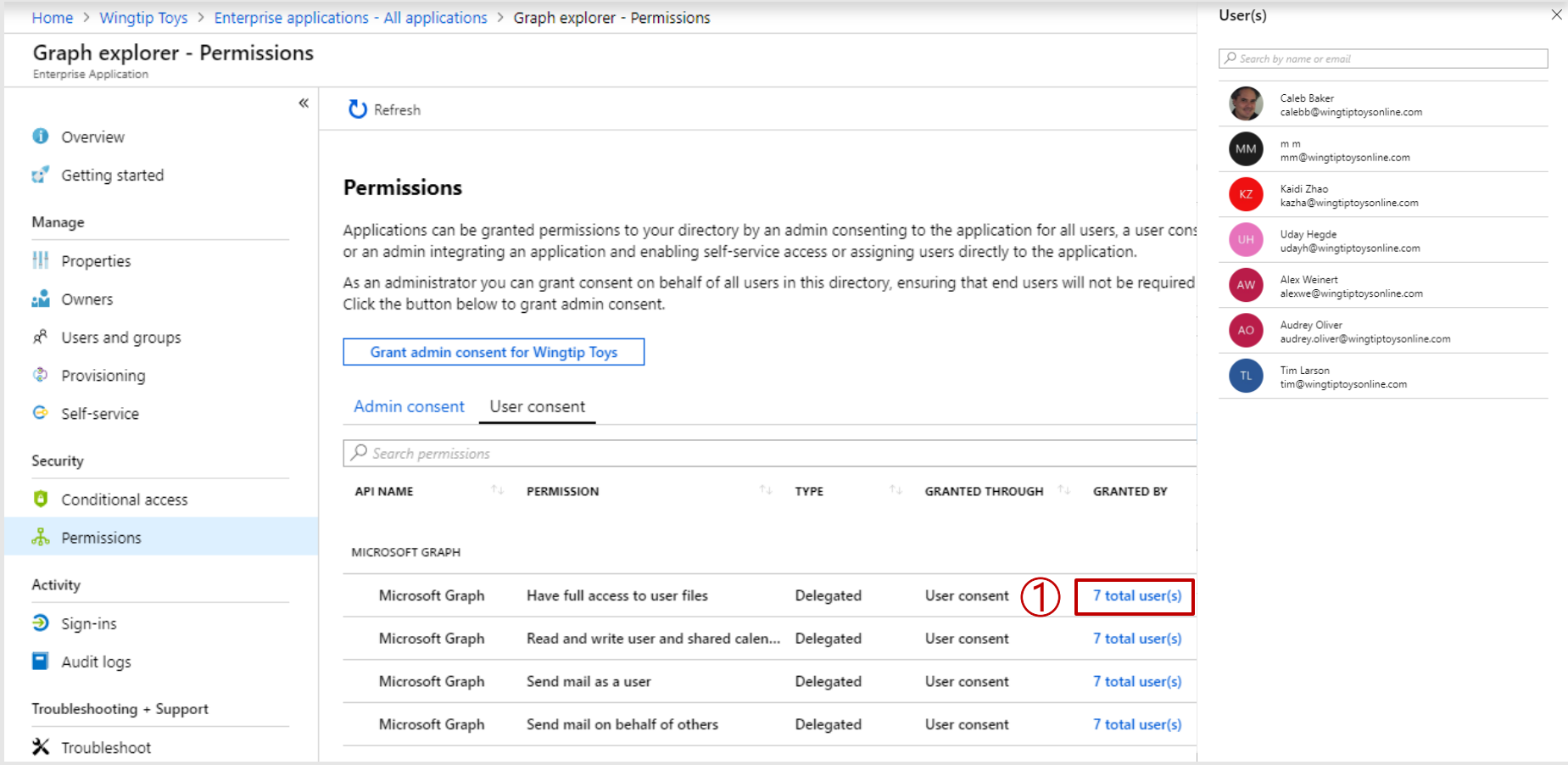
Audit consented permission for all apps

- Audit your application access and permissions that are granted
  1. Navigate to AAD -> Enterprise Apps -> identified application
  2. Select Permissions
  3. Review *Admin consent* and *User consent*



Audit user access to apps

- Audit your application access and permissions that are granted
  1. Clicking on # total user(s) brings up the users who have consented to the permission



Audit apps and consented permissions with PowerShell

Review both:

- Delegated permissions (OAuth2PermissionGrants)
- Application permissions (AppRoleAssignments).

.\Get-AzureADPSPermissions.ps1 | *Export-Csv -Path "permissions.csv" -NoTypeInformation*

Review output, especially:

- consents that are of ConsentType of 'AllPrincipals'.
- discrete permissions that each delegated permission or application has
- specific users that have consents granted. If high profile or high impact users have inappropriate consents granted, you should investigate further.
- ClientDisplayName for apps that seem suspicious.

*Courtesy of Philippe Signoret

Go Do #8

- Audit consented permissions for all applications
  - Identify potential overprivileged or risky permissions
- Audit user access to apps
  - Identify users who have access to apps but shouldn’t

Identity Secure Score

Visibility into your Identity security position and how to improve it

Insights into your Identity security position

- Easily compare score against other organizations
- View trends

Guidance to increase your security level

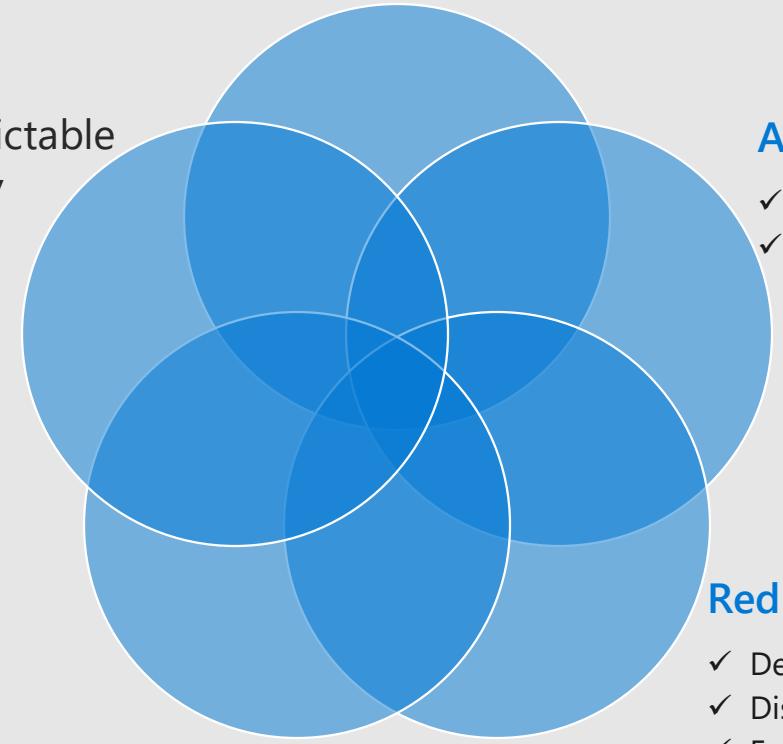
- Set an ideal score.
- Choose controls to achieve ideal score based on impact.
- Ignore controls that are not valid for you.
- 3rd party product support.

Checkout your Identity secure score now @ http://aka.ms/MyIdentitySecureScore

Identity secure score recommendations

Before we begin...

- ✓ Enable MFA for Azure AD privileged roles



Enable self-help for more predictable and complete end user security

- ✓ Enable self-service password reset

Automate threat response

- ✓ Enable sign-in risk policy
- ✓ Enable user risk policy

Strengthen your credentials

- ✓ Do not expire passwords
- ✓ Turn on Password Hash Sync if hybrid
- ✓ Enable MFA for users
- ✓ Ensure all users are registered for Multi-Factor authentication

Reduce your attack surface

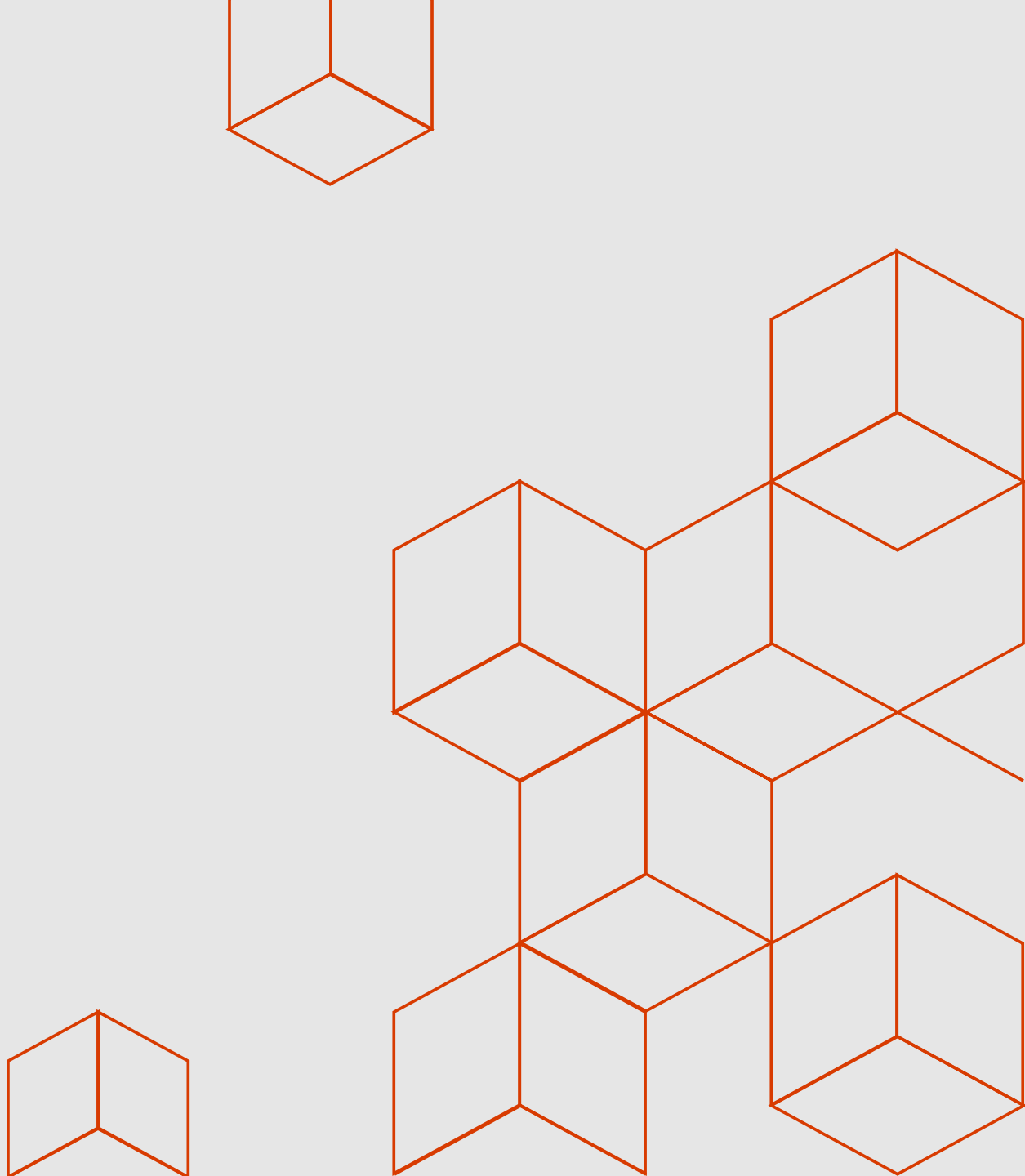
- ✓ Designate less than 5 global admins
- ✓ Disable accounts not used in last 30 days
- ✓ Enable policy to block legacy authentication
- ✓ Use non-global administrative roles
- ✓ Do not allow users to grant consent to unmanaged applications

Learn more about the 5 steps to secure your identity infrastructure: http://aka.ms/securitysteps

Go Do #9

- Use Secure Score

Secure Score



Summary: GO DOs!

TODAY:

Enable MFA for your Admin Accounts or better use PIM!

- 1.7% admins protected by MFA

Monitor your Risk Reports

Use Identity Secure Score

NEXT WEEK:

Turn on Password Hash Sync

Pull Azure AD Logs into your SIEM systems

NEXT 2 WEEKS:

Block Legacy Auth

Enable Banned Passwords

Block Suspicious IPs

NEXT MONTH:

Enable MFA for your end users

- Either CA or sign-in risk policy

Enable user risk policy

Review app permissions

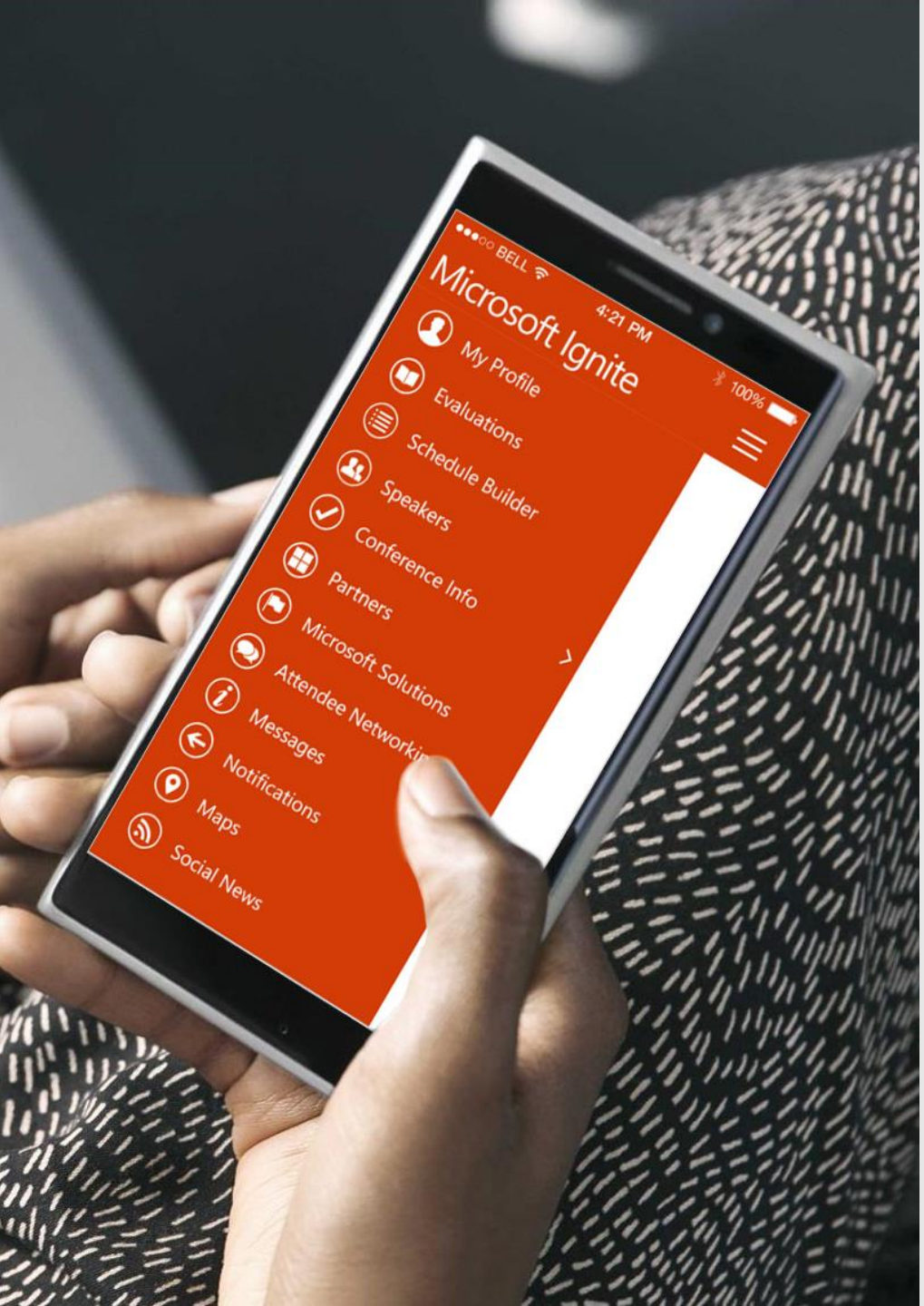
Resources

- 5 steps to secure your identity infrastructure: http://aka.ms/securitysteps
- Password guidance: Microsoft Password Guidance White Paper
- Identity Secure score: http://aka.ms/Identitysecurescoredoc
- Azure AD Data Security Whitepaper http://aka.ms/aaddatawhitepaper

Related Sessions

More breakouts, theaters, and labs
aka.ms/AADIgniteSessions

BRK3031	Getting to a world without passwords	**Tue** 12:30
BRK2252	Taking steps one, two, and three to a zero-trust network	**Tue** 12:45
BRK2369	Get apps out the door faster and easier: Microsoft's unified programming model for authentication, app management, and securely accessing APIs	**Tue** 12:30
BRK2157	Ensure comprehensive identity protection with Microsoft 365	**Wed** 9:00
BRK3241	Enable Azure Active Directory Conditional Access to secure user access while unlocking productivity across Microsoft 365	**Wed** 12:30
BRK3243	Hybrid identity and access management best practices	**Thu** 9:00
BRK3251	Shut the door to cybercrime with identity-driven security	**Thu** 10:45
BRK3240	Secure customer identity and access management using Azure Active Directory B2C	**Thu** 3:15
BRK3249	Granting partners and suppliers access to resources using Azure Active Directory B2B collaboration	**Fri** 10:45



Please evaluate this session

Your feedback is important to us!

From your PC or Tablet visit MyIgnite at http://myignite.microsoft.com

From your phone download and use the Ignite Mobile App by scanning the QR code above or visiting https://aka.ms/ignite.mobileapp