Microsoft

Microsoft Ignite The Tour

Microsoft

Move Beyond passwords – Securing your Microsoft 365 Tenant

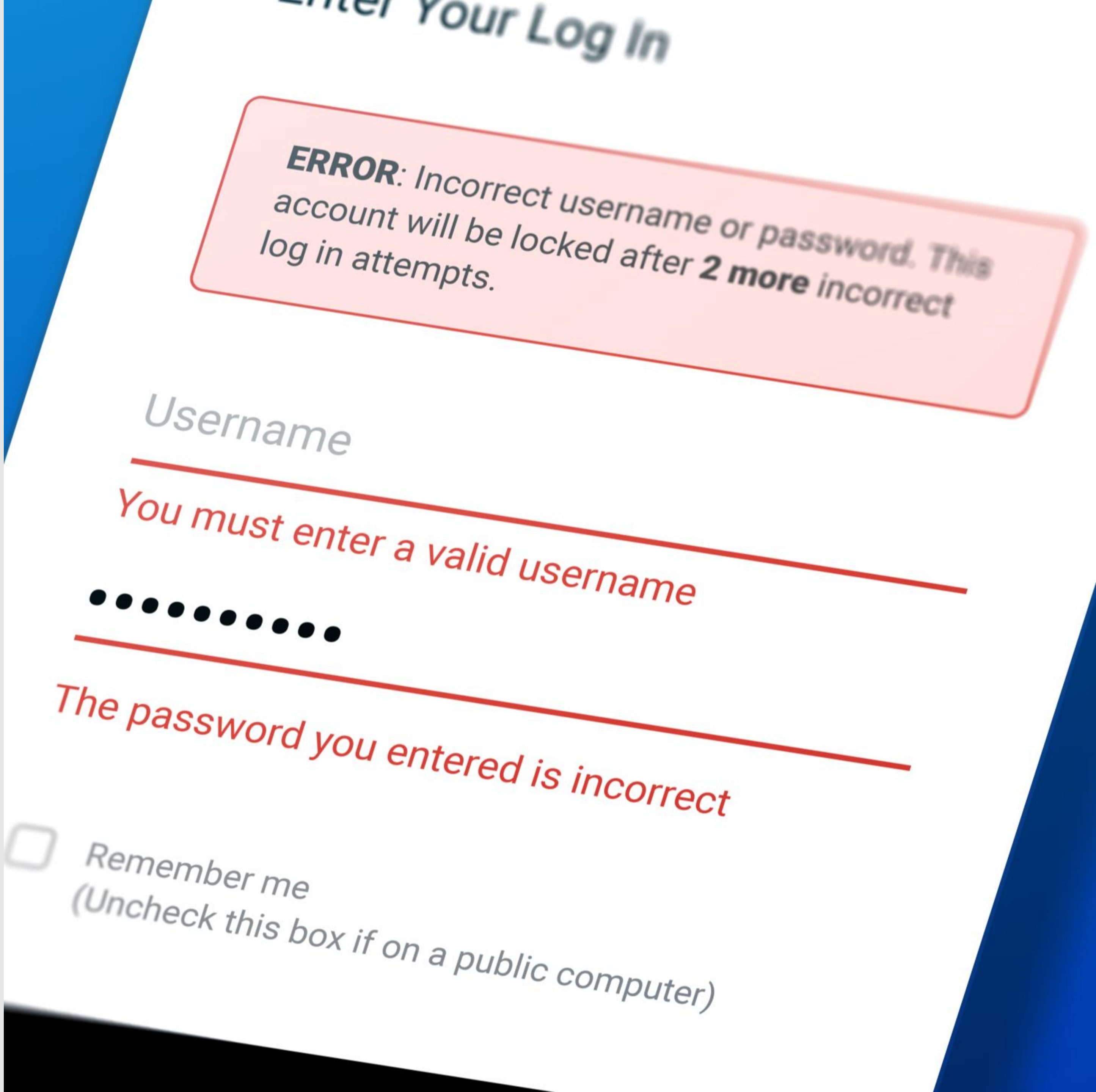
Jan Ketil Skanke
MVP Enterprise Mobility
Principal Cloud Architect – CloudWay

Twitter @JankeSkanke

Pa$$words @re 3v1l

Pa$$words @re 3v1l

Pa$$words @re 3v1l



Enter Your Log In

ERROR: Incorrect username or password. This account will be locked after **2 more** incorrect log in attempts.

Username

You must enter a valid username

••••••••••

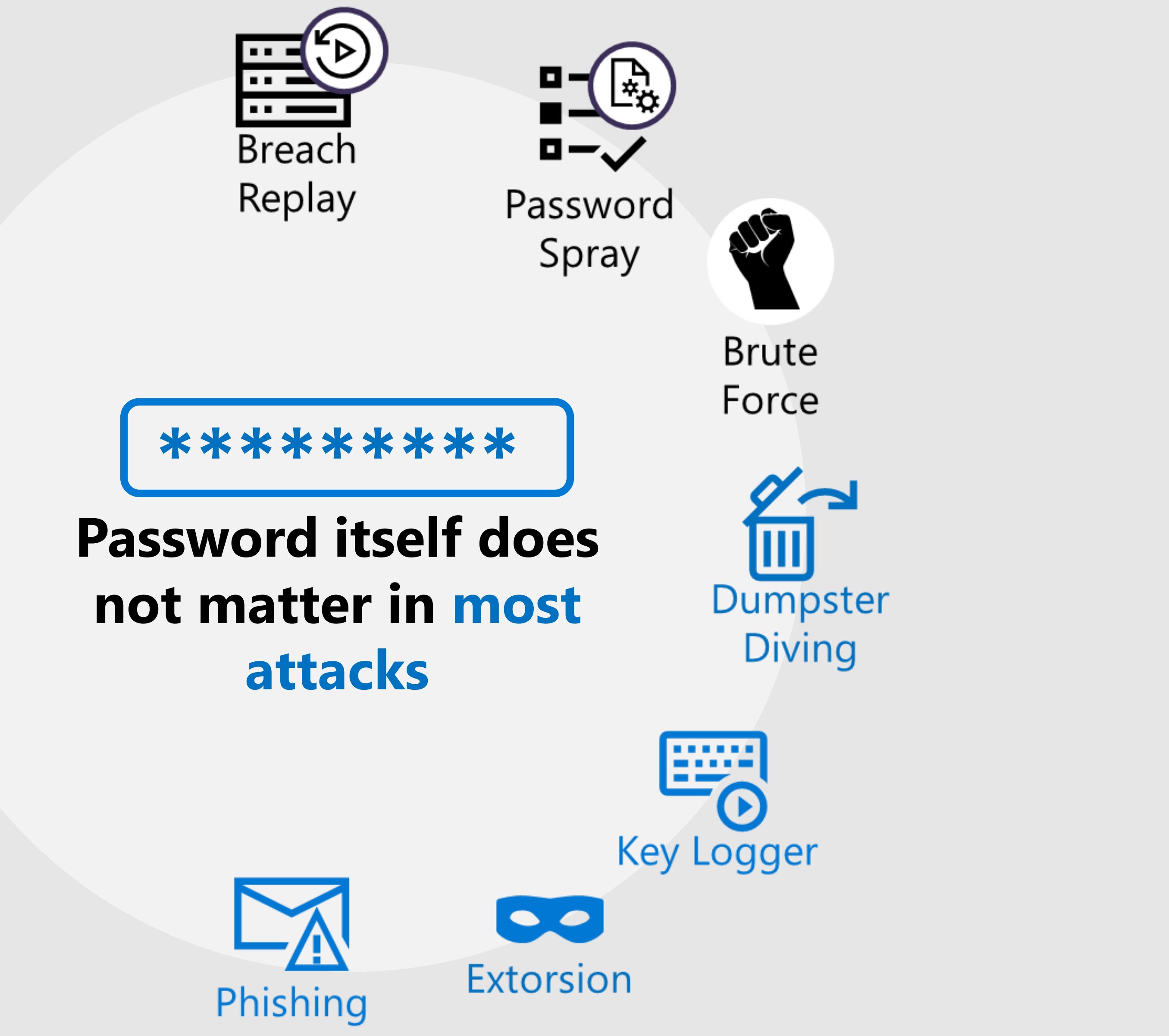
The password you entered is incorrect

□ Remember me
(Uncheck this box if on a public computer)

Everyone hates passwords?

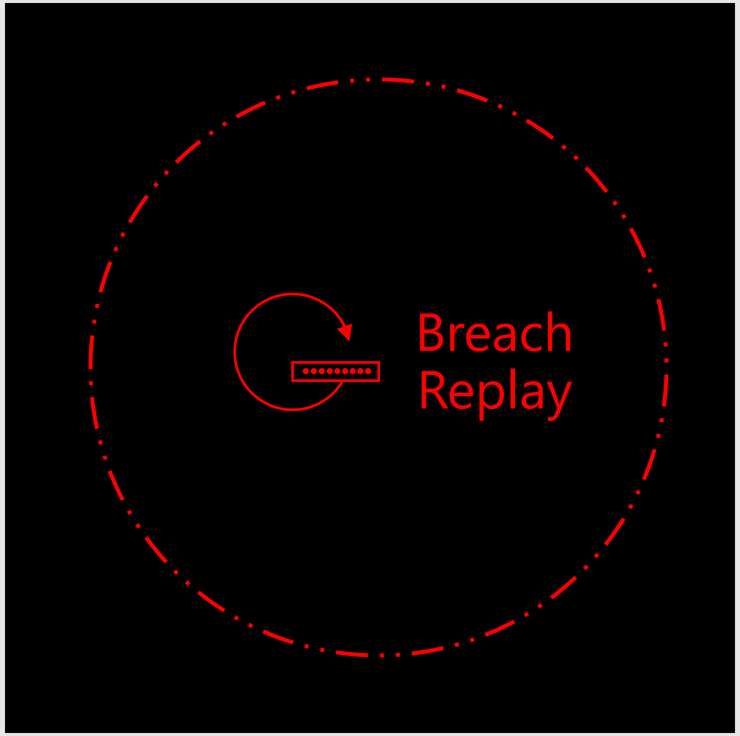
Almost everyone hates passwords

Your Pa$$words doesn't matter

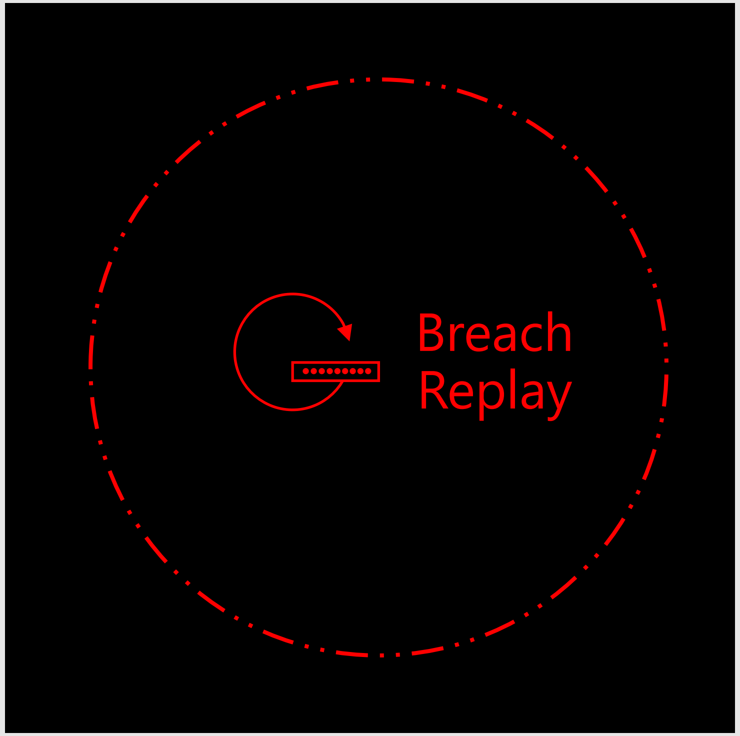


Password itself does not matter in most attacks

Your Pa$$words doesn’t matter



Your Pa$$words doesn’t matter



No,
Attacker has exact password

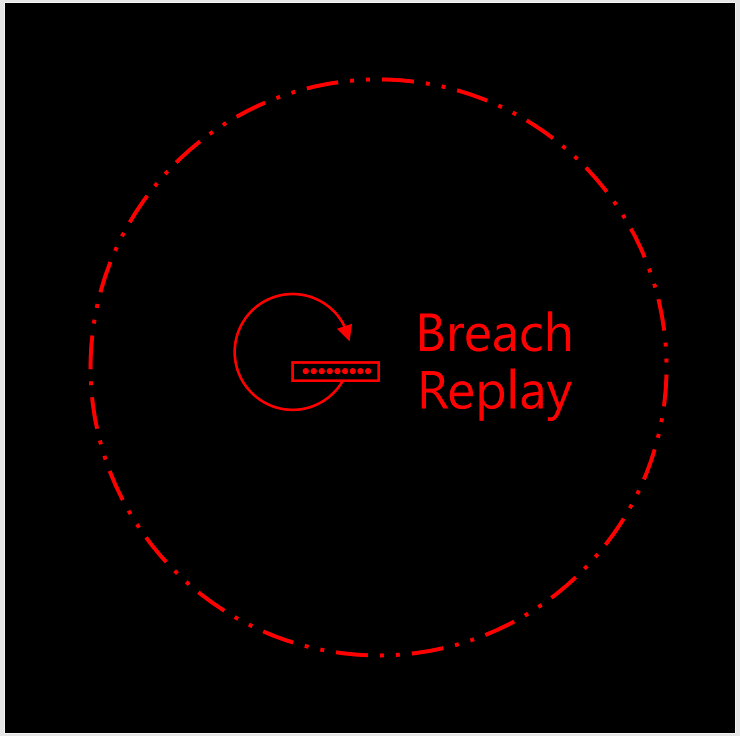
Your Pa$$words doesn’t matter

Breach Replay

Phishing

No,
Attacker has exact password

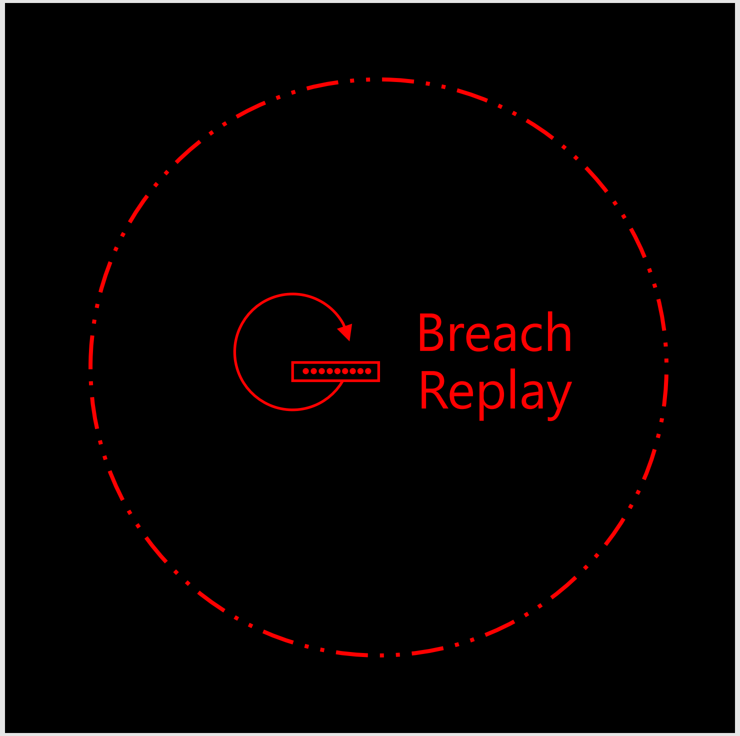
Your Pa$$words doesn’t matter



No,
Attacker has exact password

No,
User gives the password to the attacker

Your Pa$$words doesn’t matter



Breach Replay

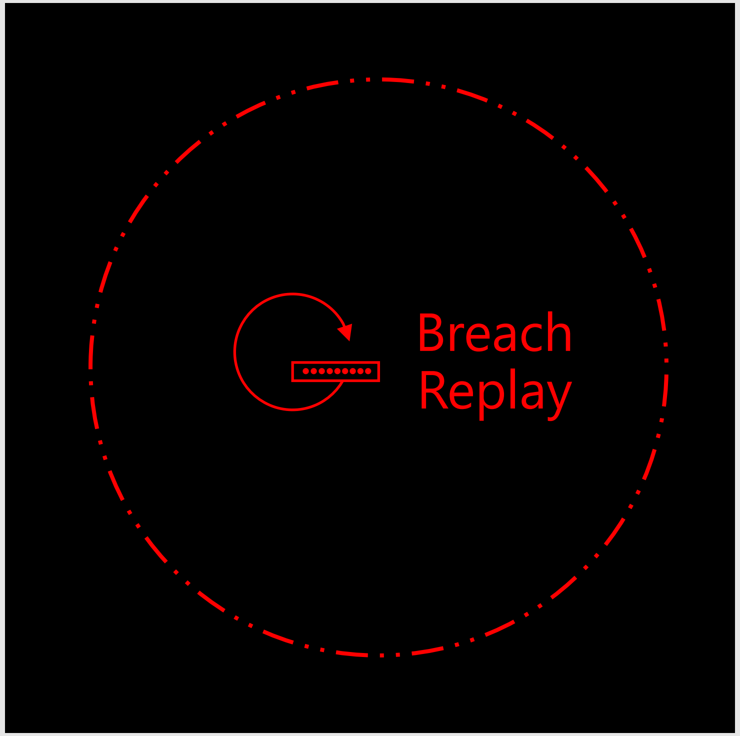
No,
Attacker has exact password

Phishing

No,
User gives the password to the attacker

Password Spray

Your Pa$$words doesn’t matter



No,
Attacker has exact password

No,
User gives the password to the attacker

No, unless
Password in top passwords list attackers are trying.

1,648,000+

Compromised accounts due to password spray
in the last 4 months

Your Pa$$words doesn’t matter

Breach Replay

4.8 Billion
Attacker driven sign-ins detected
in one month

Phishing

400%
increase in URLs discovered
from January to July 2019.

Password
Spray

1,648,000+
Compromised accounts over
4 months

Educate users

Phishing:

Watch for signs of phishing attacks. If you receive an email that looks even slightly suspicious, do the following:

- Hover over the link and look for the name of the actual website the link is sending you to
- Search for the legitimate website instead of clicking a link

Spoofing:

A message from someone you know that looks a bit unusual could mean the sender's email account was compromised. Contact the sender and ask if it was legitimate.

Passwords:

Never reuse passwords or share accounts with coworkers.

Educate users to create good passwords

How many admins do you think have enabled MFA?

It’s getting better … still bad

MFA your privileged accounts

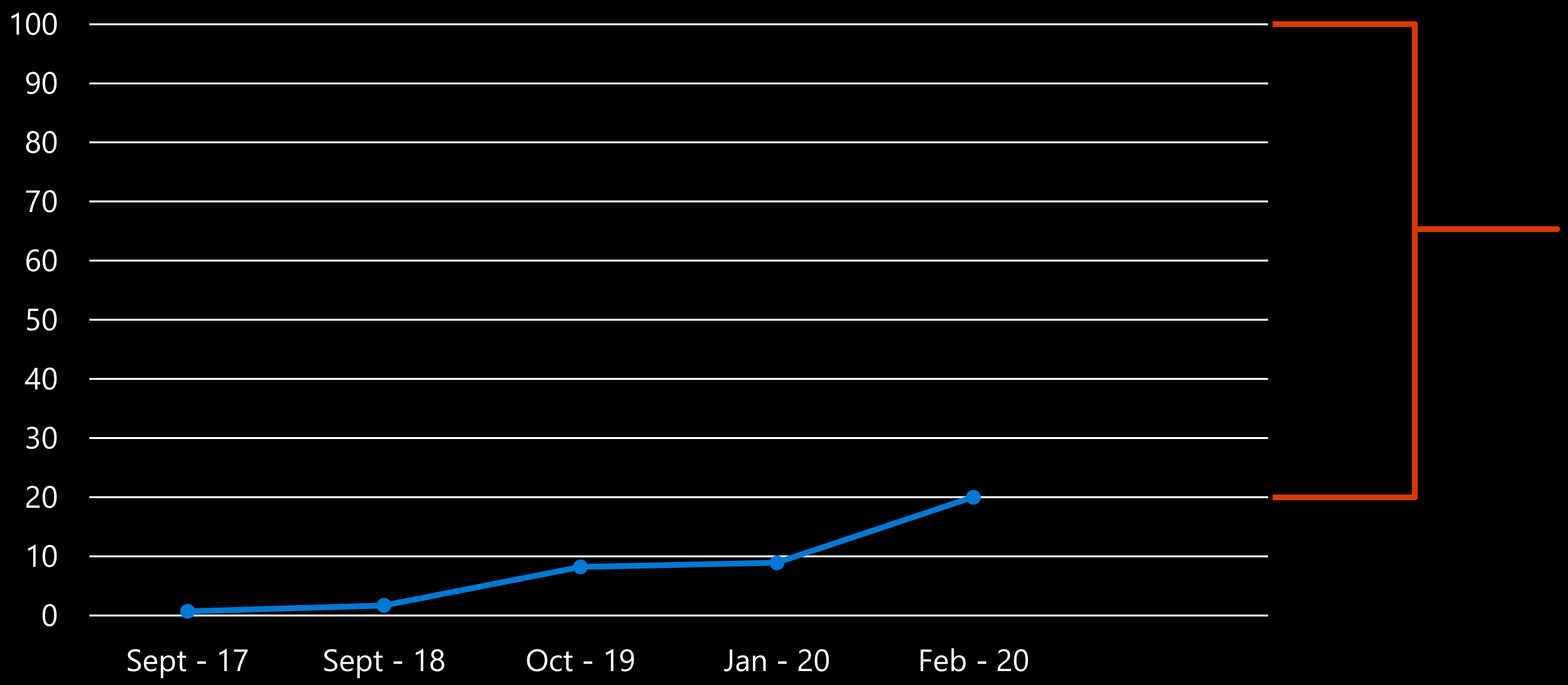
Sep 2017: 0.7%

Sep 2018: 1.7%

Oct 2019: 8.2%

Feb 2020 20+ %

Percentage of Admins with MFA



80% of admins without MFA

Enable MFA

Today!

Enable MFA Right for All Users

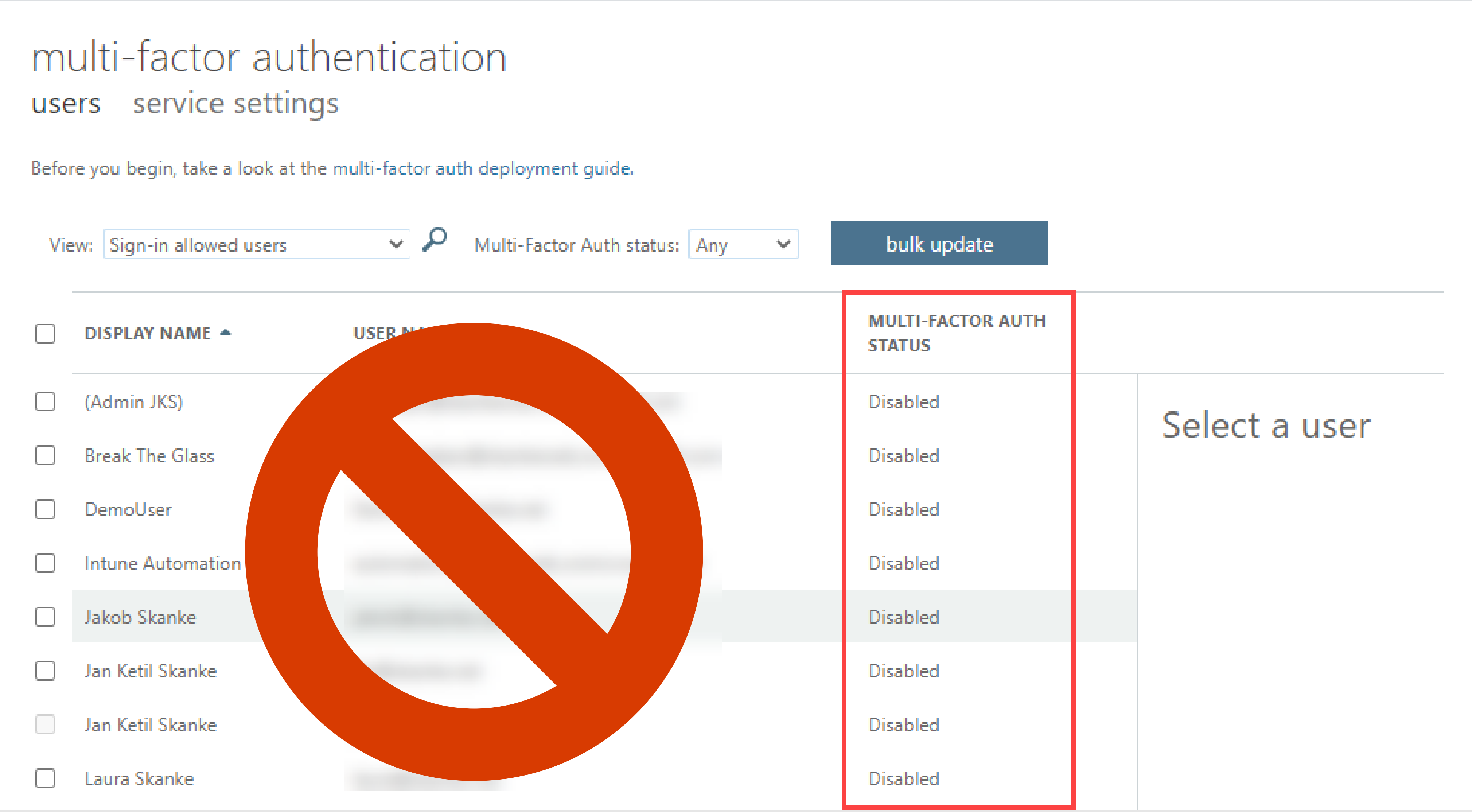
1. Do not enable MFA on a per user basis in Users pane of the Admin Center
2. Disable Basic Auth
3. Break the Glass Account for emergencies
4. Protect All your Admins – All the time
5. Use Conditional Access
6. Utilize Microsoft Endpoint Manager for Compliant Devices

1

Do not enable MFA on a per user level

MFA Setup

1



multi-factor authentication

users   service settings

Before you begin, take a look at the multi-factor auth deployment guide.

View: Sign-in allowed users   Multi-Factor Auth status: Any

☐	DISPLAY NAME ▲	USER N	MULTI-FACTOR AUTH STATUS
☐	(Admin JKS)	[redacted]	Disabled
☐	Break The Glass	[redacted]	Disabled
☐	DemoUser	[redacted]	Disabled
☐	Intune Automation	[redacted]	Disabled
☐	Jakob Skanke	[redacted]	Disabled
☐	Jan Ketil Skanke	[redacted]	Disabled
☐	Jan Ketil Skanke	[redacted]	Disabled
☐	Laura Skanke	[redacted]	Disabled

Select a user

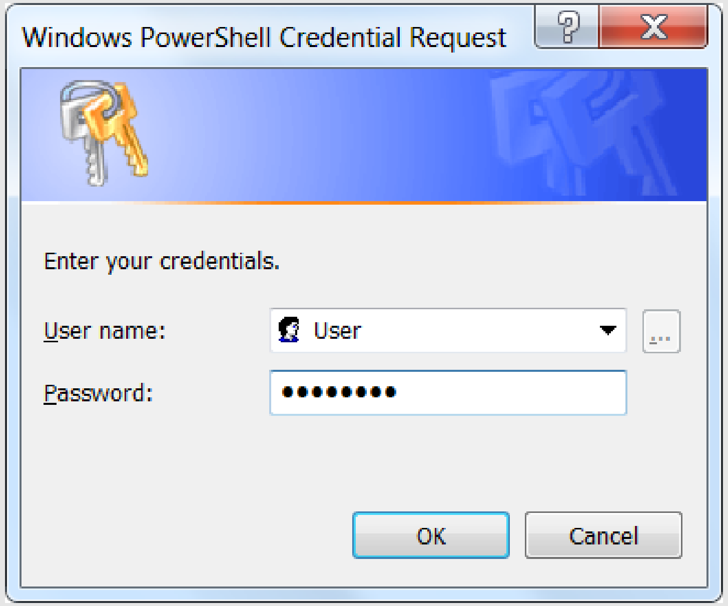
2

Disable Basic Auth

Disable Basic Auth

2

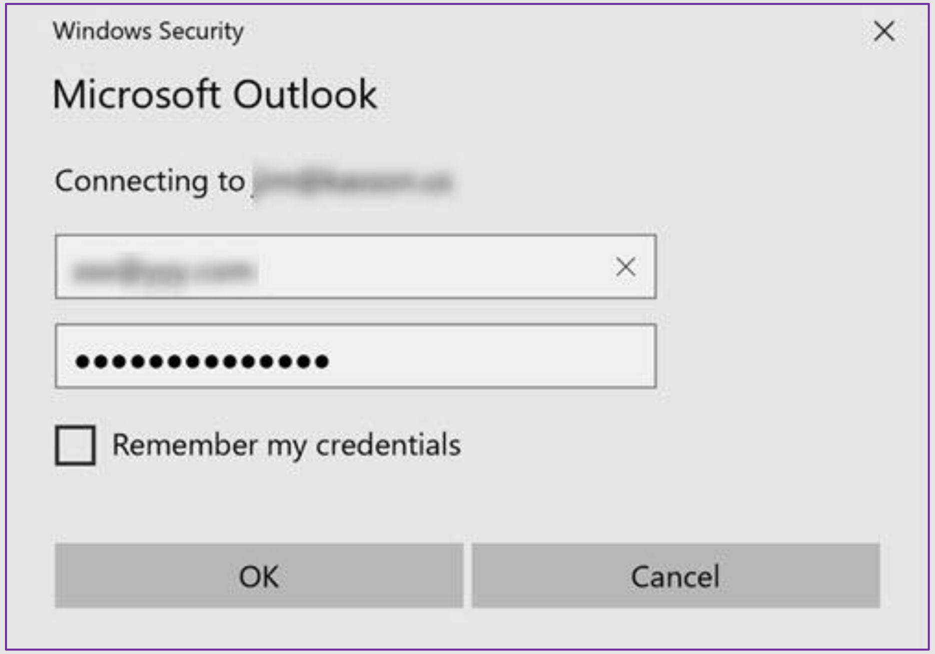
Examples of Basic Auth


Windows PowerShell Credential Request

Enter your credentials.

User name: User

Password: ••••••••


Windows Security

Microsoft Outlook

Connecting to [redacted]

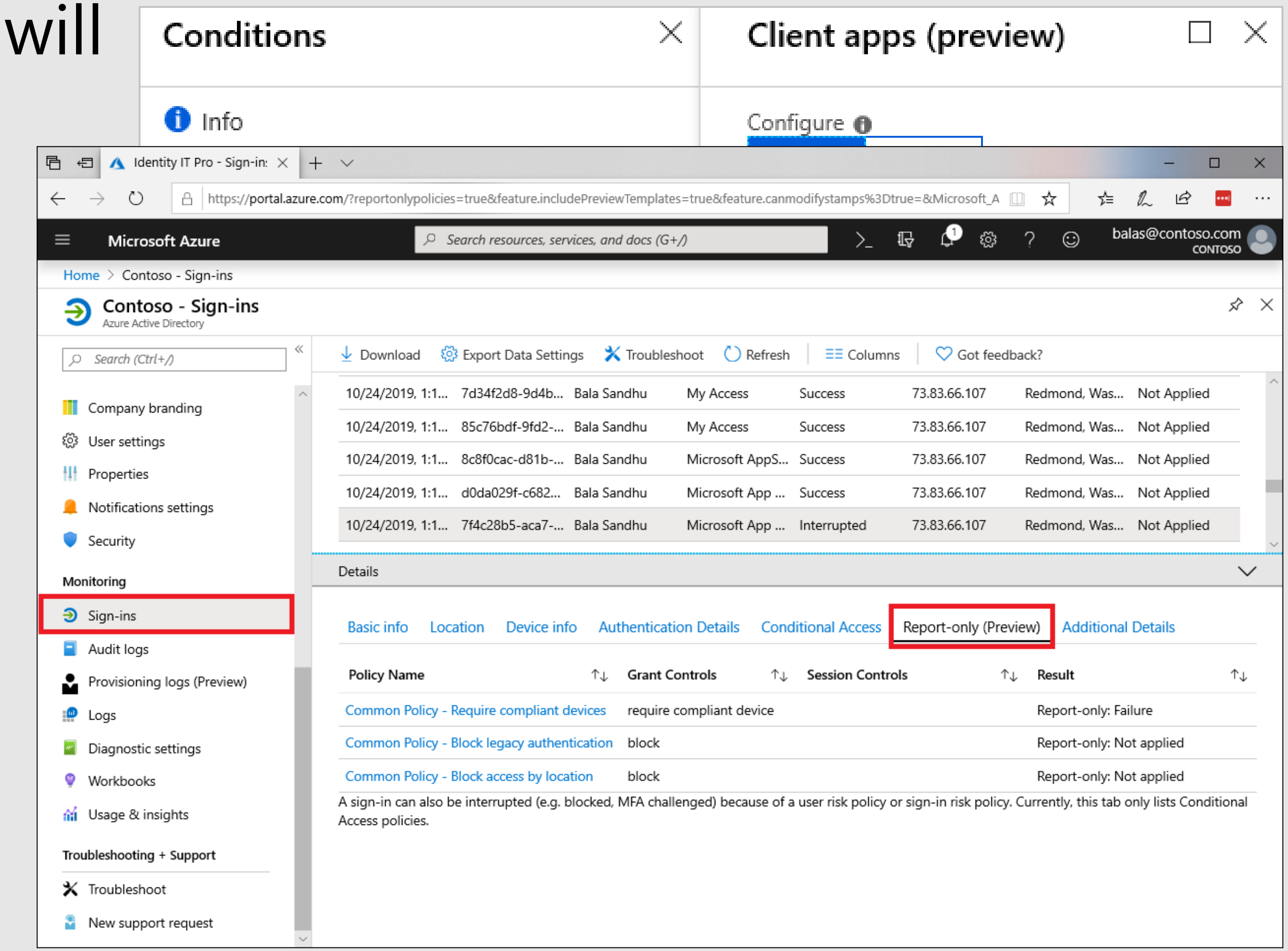
[redacted]

•••••••••••••••

□ Remember my credentials

Blocking Legacy Authentication In Azure AD

- Conditional Access policies will block post-authentication
- Report-only mode can help measure the impact



https://portal.azure.com/?reportonlypolicies=true&feature.includePreviewTemplates=true&feature.canmodifystamps%3Dtrue=&Microsoft_A

10/24/2019, 1:1...	7d34f2d8-9d4b...	Bala Sandhu	My Access	Success	73.83.66.107	Redmond, Was...	Not Applied
10/24/2019, 1:1...	85c76bdf-9fd2-...	Bala Sandhu	My Access	Success	73.83.66.107	Redmond, Was...	Not Applied
10/24/2019, 1:1...	8c8f0cac-d81b-...	Bala Sandhu	Microsoft AppS...	Success	73.83.66.107	Redmond, Was...	Not Applied
10/24/2019, 1:1...	d0da029f-c682...	Bala Sandhu	Microsoft App ...	Success	73.83.66.107	Redmond, Was...	Not Applied
10/24/2019, 1:1...	7f4c28b5-aca7-...	Bala Sandhu	Microsoft App ...	Interrupted	73.83.66.107	Redmond, Was...	Not Applied

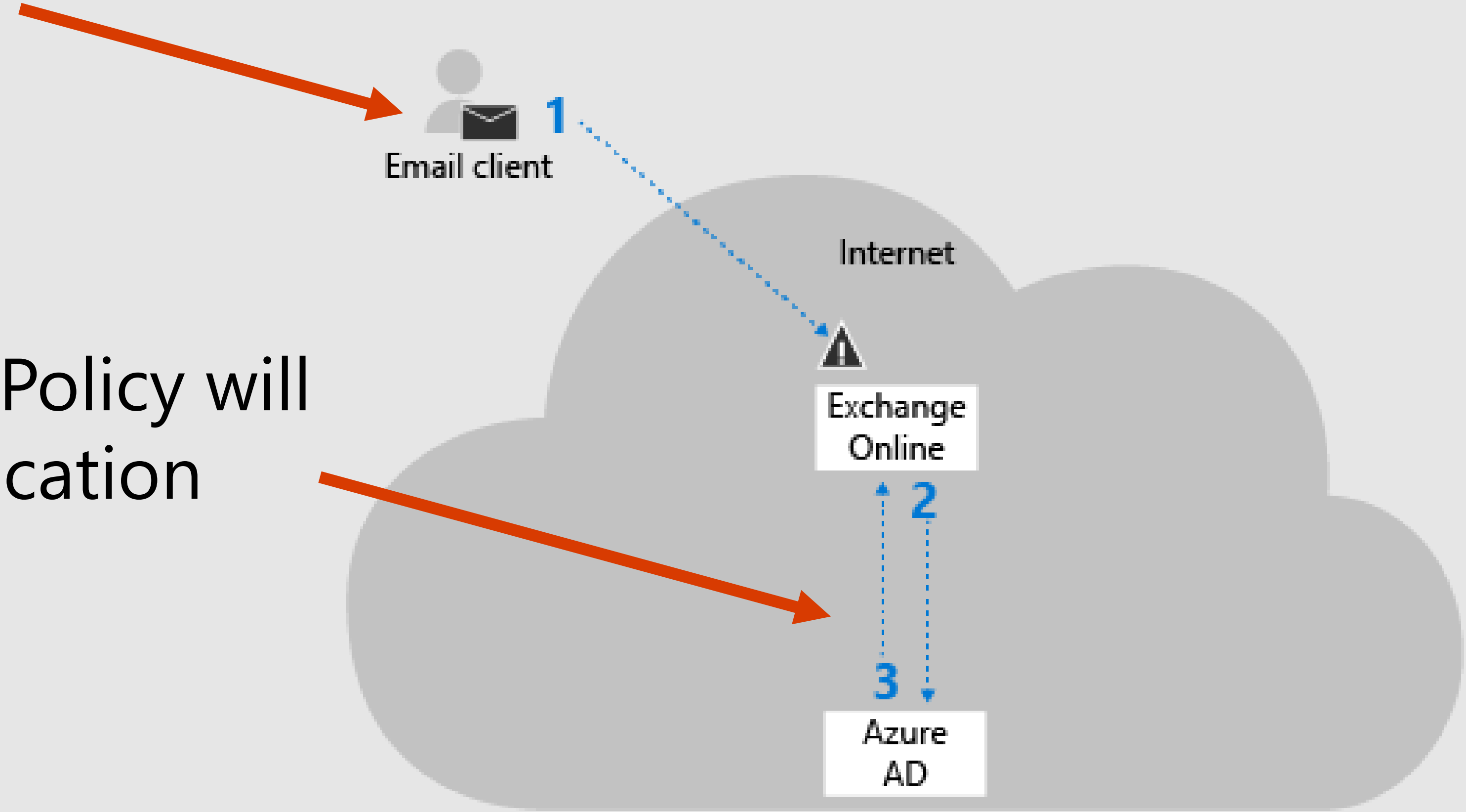
Policy Name	Grant Controls	Session Controls	Result
Common Policy - Require compliant devices	require compliant device		Report-only: Failure
Common Policy - Block legacy authentication	block		Report-only: Not applied
Common Policy - Block access by location	block		Report-only: Not applied

A sign-in can also be interrupted (e.g. blocked, MFA challenged) because of a user risk policy or sign-in risk policy. Currently, this tab only lists Conditional Access policies.

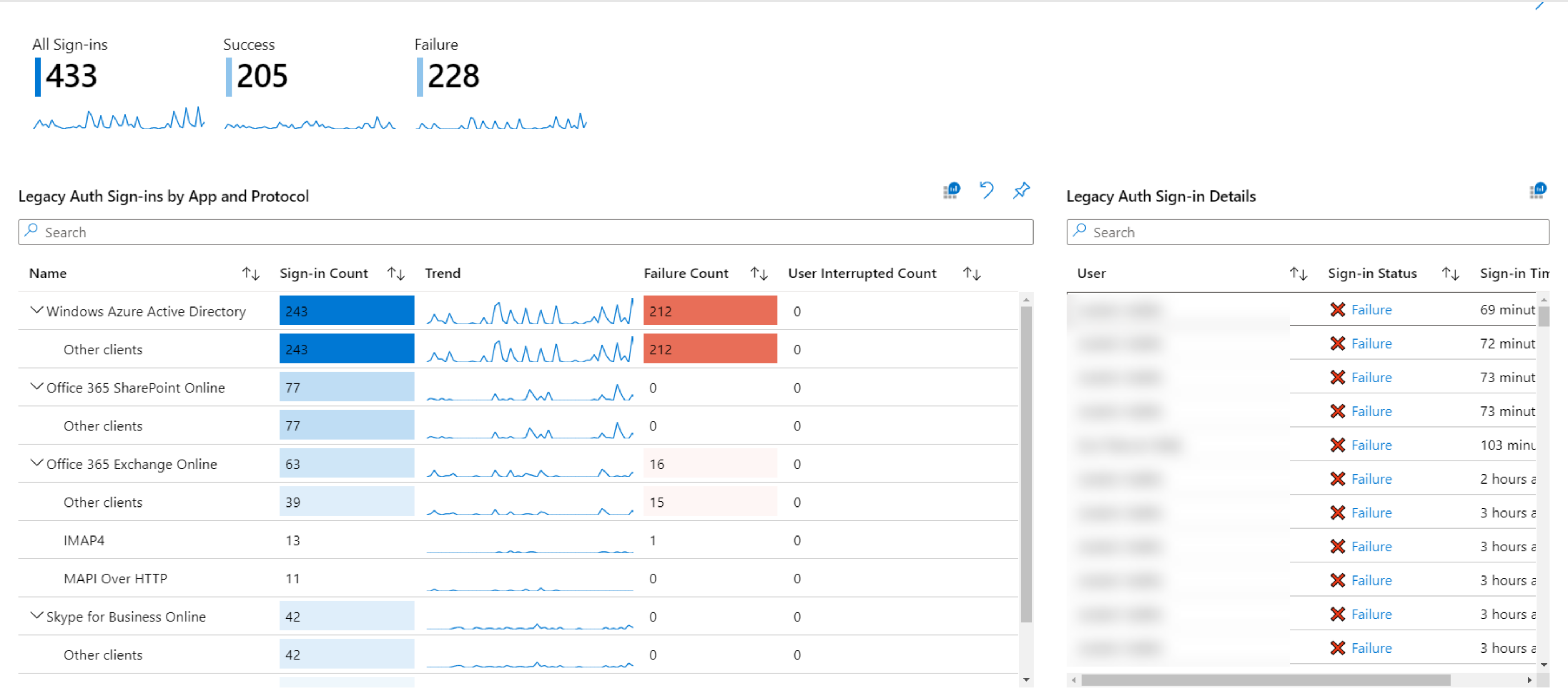
Blocking Basic Authentication

- Exchange Online Authentication Policy will block pre-authentication

- Conditional Access Policy will block post-authentication



Find Legacy Authentication



All Sign-ins 433

Success 205

Failure 228

Legacy Auth Sign-ins by App and Protocol

Search

Name	Sign-in Count	Trend	Failure Count	User Interrupted Count
Windows Azure Active Directory	243		212	0
Other clients	243		212	0
Office 365 SharePoint Online	77		0	0
Other clients	77		0	0
Office 365 Exchange Online	63		16	0
Other clients	39		15	0
IMAP4	13		1	0
MAPI Over HTTP	11		0	0
Skype for Business Online	42		0	0
Other clients	42		0	0

Legacy Auth Sign-in Details

Search

User	Sign-in Status	Sign-in Tim
[redacted]	✗ Failure	69 minut
[redacted]	✗ Failure	72 minut
[redacted]	✗ Failure	73 minut
[redacted]	✗ Failure	73 minut
[redacted]	✗ Failure	103 minu
[redacted]	✗ Failure	2 hours a
[redacted]	✗ Failure	3 hours a
[redacted]	✗ Failure	3 hours a
[redacted]	✗ Failure	3 hours a
[redacted]	✗ Failure	3 hours a
[redacted]	✗ Failure	3 hours a

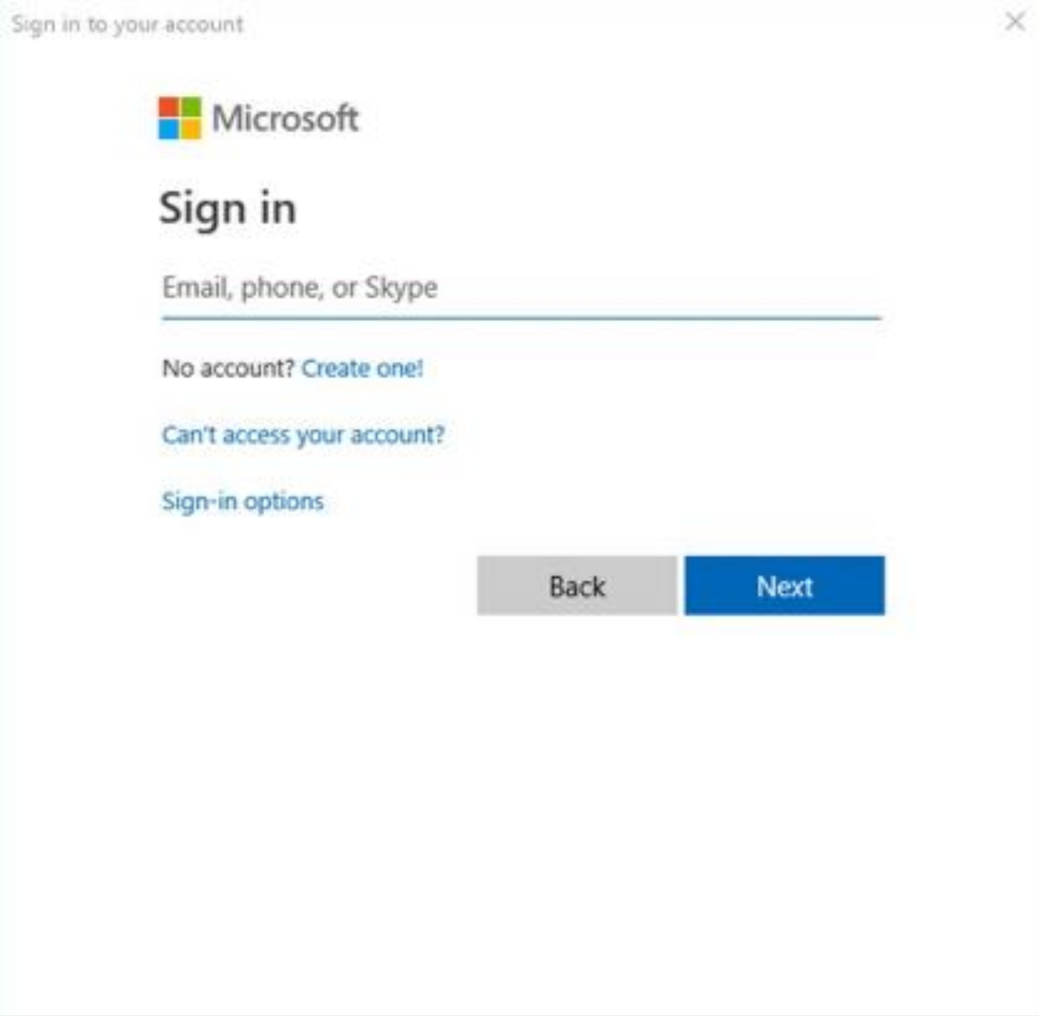
Why is Blocking Legacy auth so important?

- Turn Off Legacy Authentication
  - Cause of nearly 100% of password spray attacks
  - Reduces compromise rate by 66%

- It’s being disabled Oct 13th, 2020 in EXO!
- Does not handle additional methods or challenge

Modern Authentication

- More tools to protect resources
- Ability to handle an MFA challenge/response
- Can include additional information about the device (Hybrid Domain Join)
- Applies to mobile devices as well (MAM Policies)
- More information an attacker must guess correctly to spoof (this is good news for us!)
  - User Agent, Application Target


Sign in to your account

Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Sign-in options

3

Create
Break the Glass Account

Break the Glass Account

3

Why

- MFA Solution Down
- Network/Mobile outage
- The “Admin” leaves company
- Other

How

- Cloud Only Account
- Not Personal
- No Conditional Access
- No Password Expiry
- Global Admin
- Monitor Usage

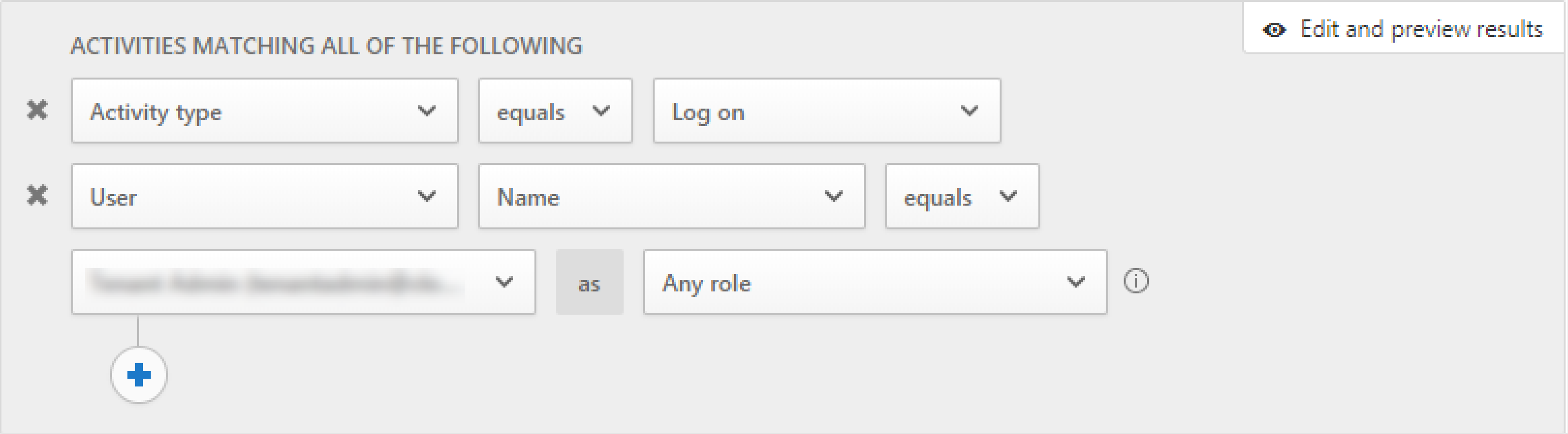
Monitor the Break the Glass Account

3

- GOOD: Azure Monitor Log Search Alert

```
SigninLogs
| where UserPrincipalName == “mybreakglassadmin@domain.com"
| project AppDisplayName , IPAddress , Location , UserPrincipalName , TimeGenerated
```

- BETTER: Microsoft Cloud App Security



Edit and preview results

ACTIVITIES MATCHING ALL OF THE FOLLOWING

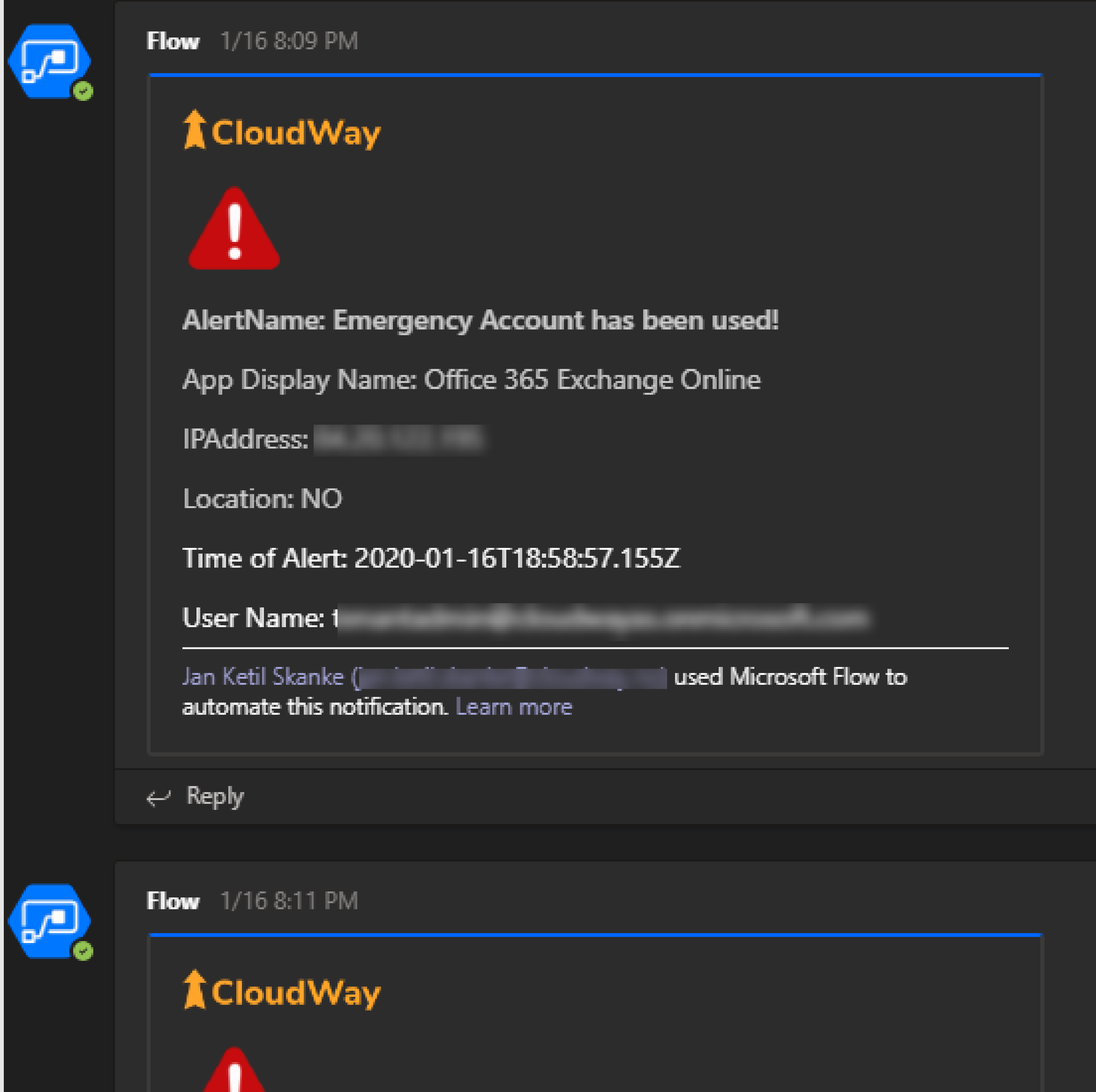
✖ Activity type | equals | Log on

✖ User | Name | equals

[redacted] as Any role

What we do:

Forward alerts to Microsoft Teams



Flow 1/16 8:09 PM

CloudWay

AlertName: Emergency Account has been used!

App Display Name: Office 365 Exchange Online

IPAddress: [redacted]

Location: NO

Time of Alert: 2020-01-16T18:58:57.155Z

User Name: t[redacted]

Jan Ketil Skanke ([redacted]) used Microsoft Flow to automate this notification. Learn more

Flow 1/16 8:11 PM

CloudWay

4

Protect All Admins

Always

4

How To Enable MFA For Your Admins

Good: Turn MFA on!

Better: Conditional Access

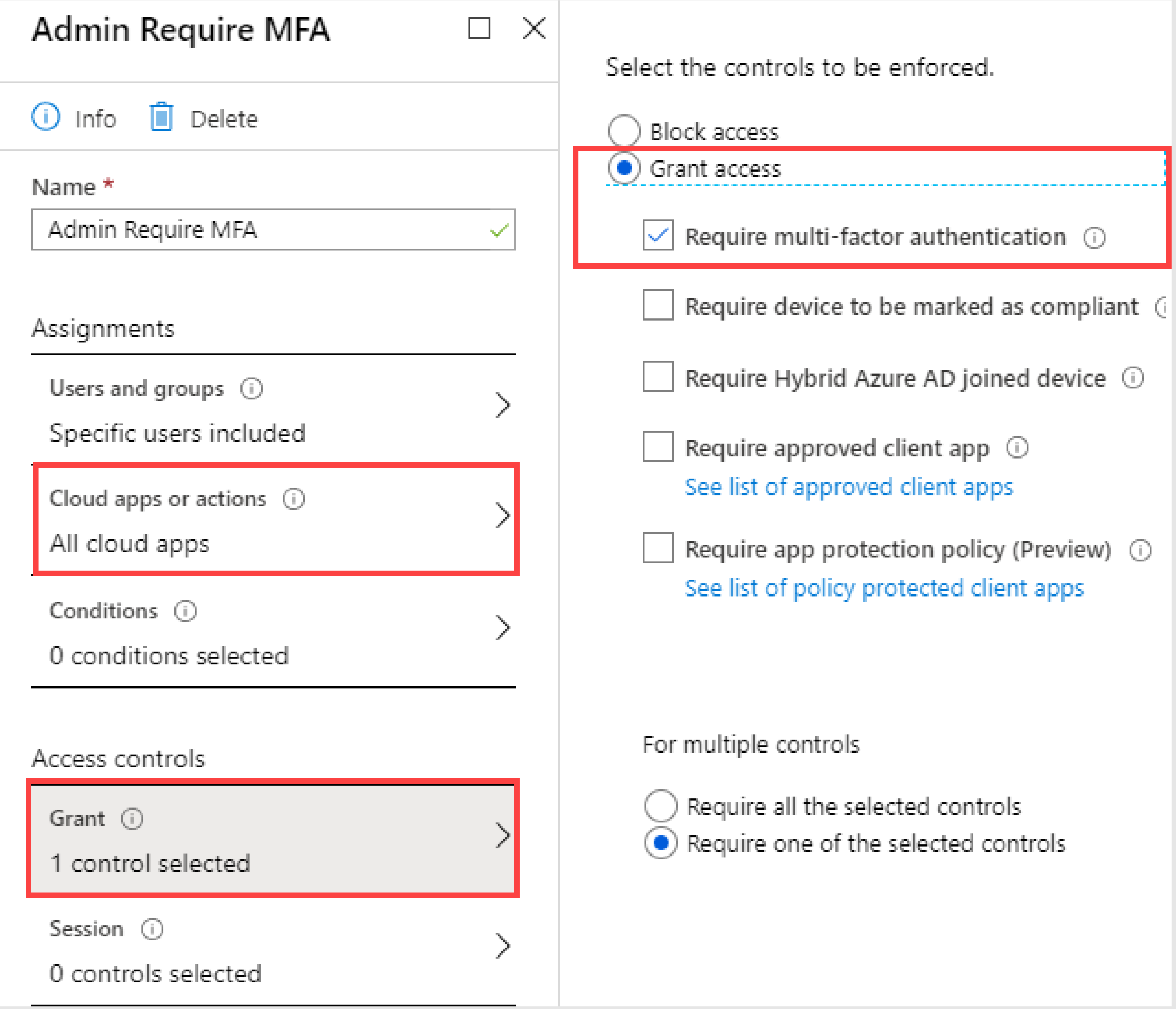
Best: Azure AD Privileged Identity Management

- No standing admin access
- Admin access requires elevation + MFA
- Approval workflows and elevation scheduling
- Alerts on admin activity taking place outside of PIM
- Applies to and protects Azure Resources as well!
- Can buy Azure AD P2 license for just your admins

Conditional Access – Require MFA

4

- Target All Privileged Accounts
- All Cloud Apps
- No exeptions
- Don’t trust network
- Require MFA Always



Admin Require MFA

Name *

Admin Require MFA

Assignments

Users and groups
Specific users included

Cloud apps or actions
All cloud apps

Conditions
0 conditions selected

Access controls

Grant
1 control selected

Session
0 controls selected

Select the controls to be enforced.

○ Block access
● Grant access

☑ Require multi-factor authentication

□ Require device to be marked as compliant

□ Require Hybrid Azure AD joined device

□ Require approved client app
See list of approved client apps

□ Require app protection policy (Preview)
See list of policy protected client apps

For multiple controls

○ Require all the selected controls
● Require one of the selected controls

5

Use Conditional Access

Conditional Access for your End Users

Secure a good user experience

5

- Require Compliant Device / Hybrid AD Join on Windows
- Require Compliant Device / App for iOS and Android
- Don’t put trust on your network
- Block unsupported platforms
- Include All Cloud Apps
- Full Block of Basic Auth

6

MS Endpoint Manager

Compliant Device

Establish Basic Device Trust for Windows

6

Intune (for cloud-first environments)	Create compliance policies Create configuration policies
SCCM and Intune co-managed (for hybrid environments)	Move Compliance Workload to Intune Create Compliance Polices in Intune
No management solution, or 3rd party management	Trust on Hybrid AD Join only (Basic) Enroll to Intune via GPO (Recommended)

Device trust also on other platforms

6

IOS

ANDROID

MAC

Enhance your security

Enhance your security

1. Always have dedicated Admins (Cloud Only)
2. Use Azure AD Identity Protection for User Risks
3. Use Microsft Defender ATP for Device Risk
4. Go Passwordless

Dedicated Admins in Cloud

Separated Cloud / On-Premises security boundaries

Avoid on-premises attacks moving to the cloud and vice versa

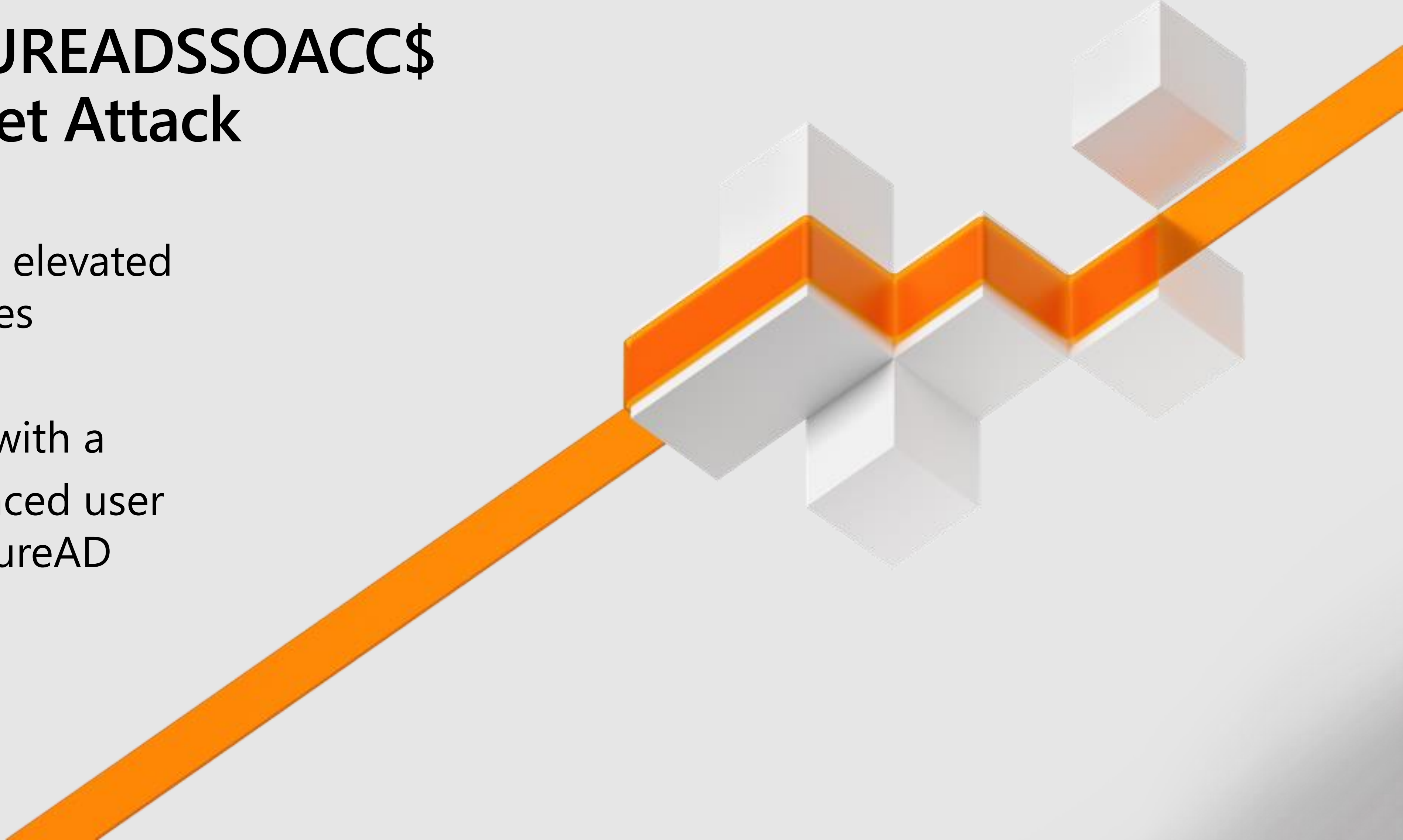
Seamless SSO (AAZUREADSSO$ Account) could be exploited

DEMO
Exploiting AZUREADSSOACC$ in a Silver Ticket Attack

Attacker has reached elevated privileges on-premises

Moves to the Cloud with a

Silver Ticket for a synced user with GA Rights in AzureAD

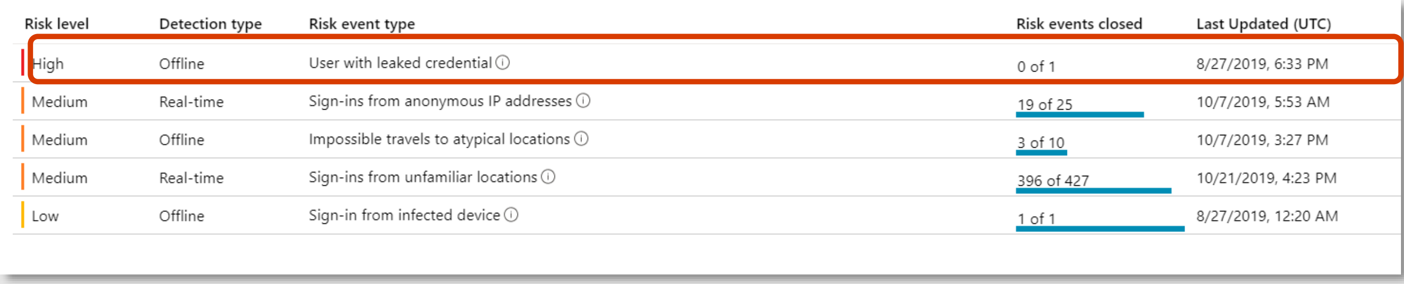


Demo:
Using the credentials on a random machine!

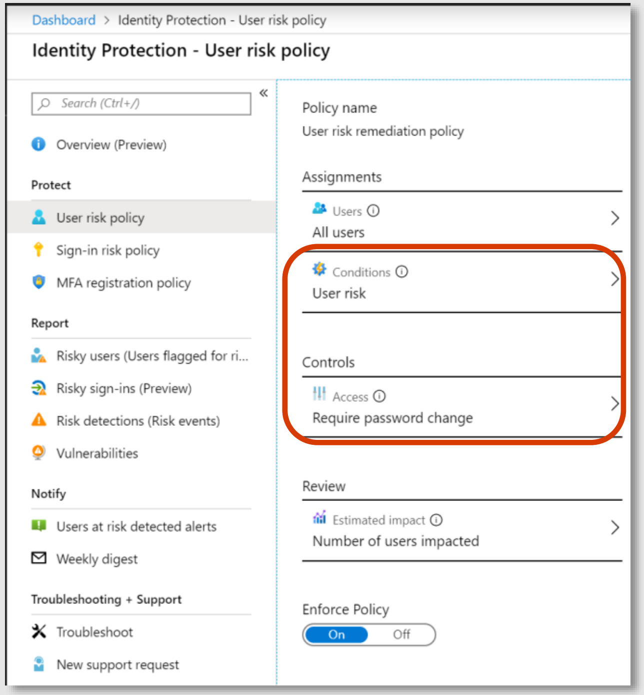
Azure AD Identity Protection

Detecting Leaked Passwords

- Microsoft monitors leaked username/passwords
- Matches generate a high-risk detection if you turned on PHS
- Azure AD Identity Protection policies automate response



Risk level	Detection type	Risk event type	Risk events closed	Last Updated (UTC)
High	Offline	User with leaked credential ⓘ	0 of 1	8/27/2019, 6:33 PM
Medium	Real-time	Sign-ins from anonymous IP addresses ⓘ	19 of 25	10/7/2019, 5:53 AM
Medium	Offline	Impossible travels to atypical locations ⓘ	3 of 10	10/7/2019, 3:27 PM
Medium	Real-time	Sign-ins from unfamiliar locations ⓘ	396 of 427	10/21/2019, 4:23 PM
Low	Offline	Sign-in from infected device ⓘ	1 of 1	8/27/2019, 12:20 AM



Dashboard > Identity Protection - User risk policy

Identity Protection - User risk policy

Policy name
User risk remediation policy

Assignments

Users ⓘ
All users

Conditions ⓘ
User risk

Controls

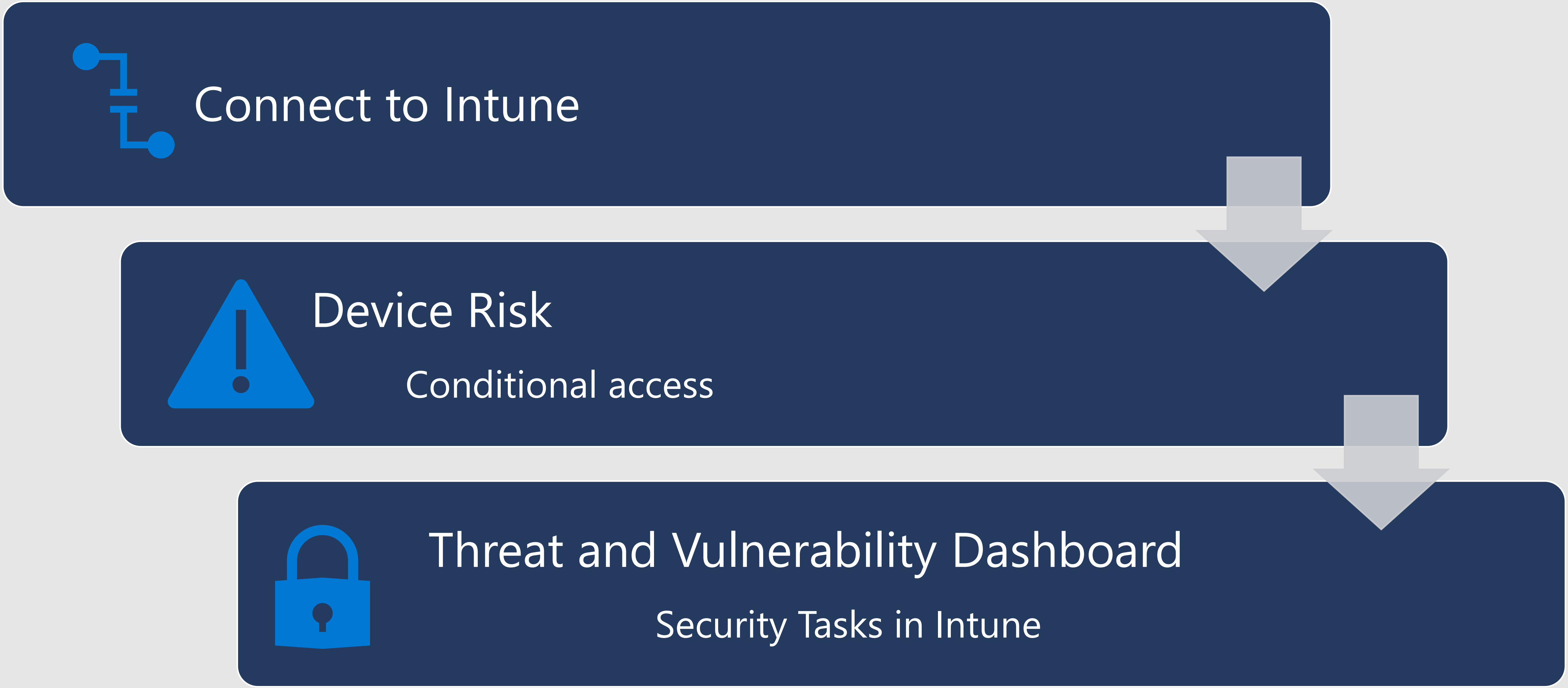
Access ⓘ
Require password change

Review

Estimated impact ⓘ
Number of users impacted

Enforce Policy
On | Off

Microsoft Defender ATP + Intune: Basics



Connect to Intune

Device Risk

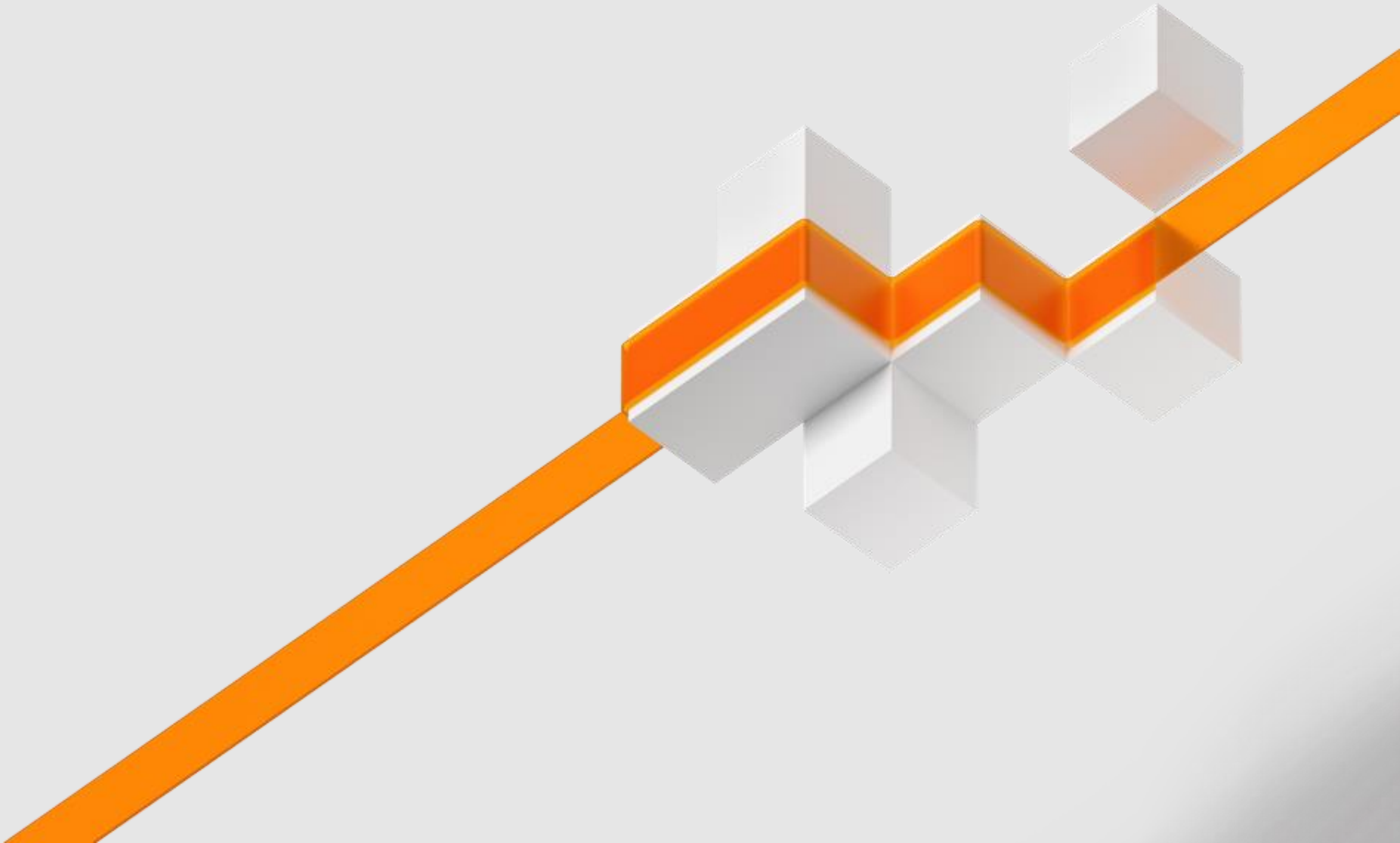
Conditional access

Threat and Vulnerability Dashboard

Security Tasks in Intune

Demo

Computer With Risk

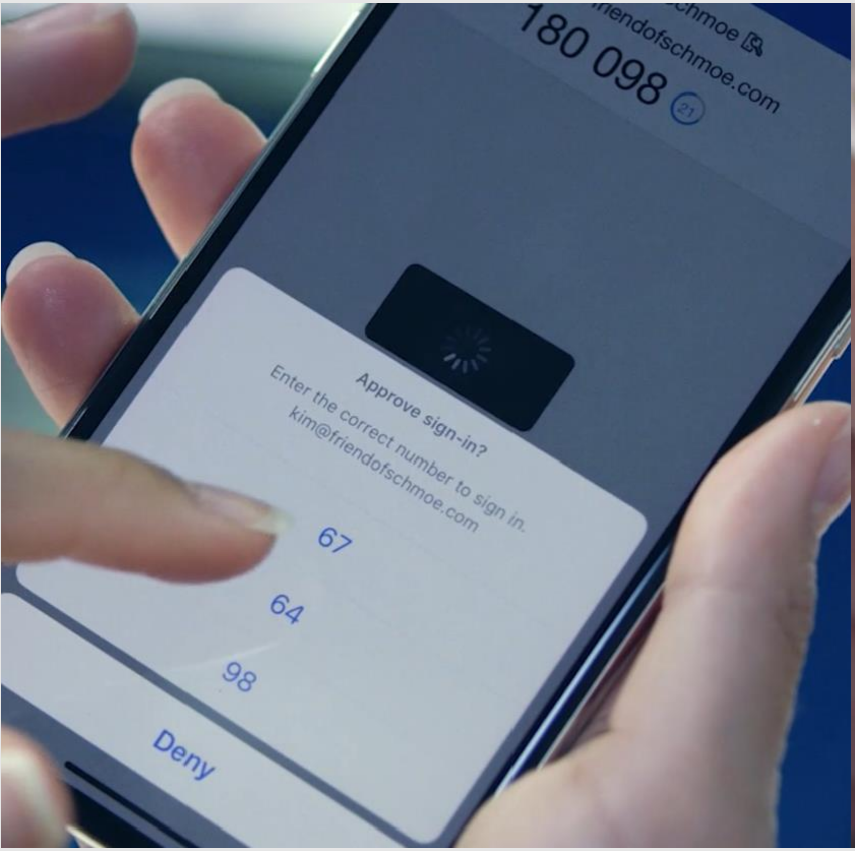


What is passwordless?

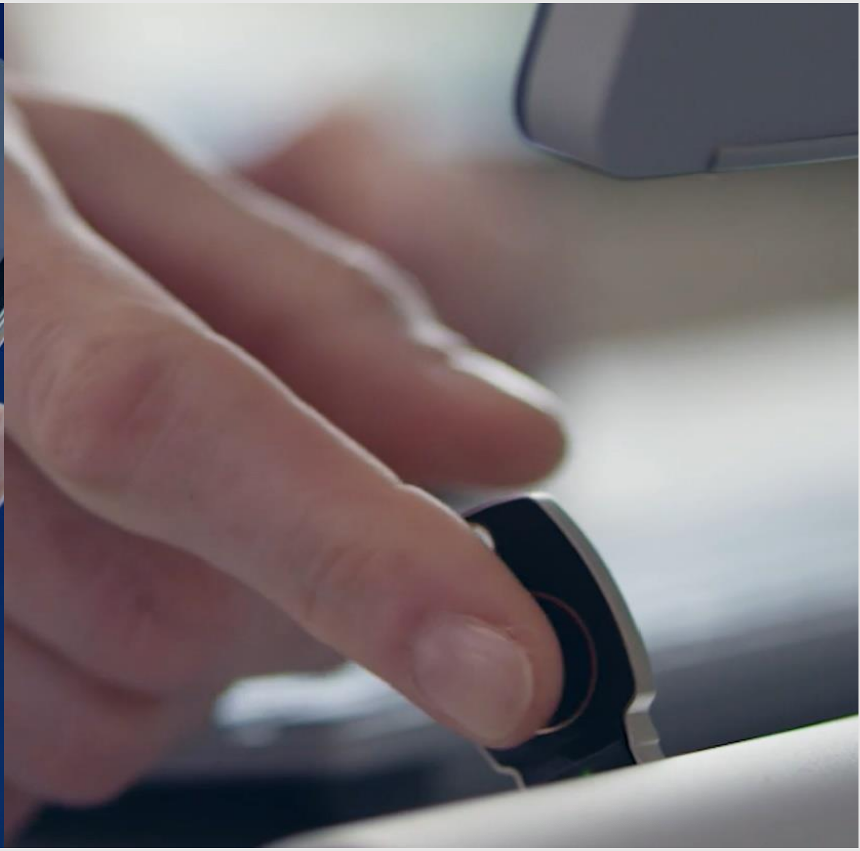
High security, convenient methods of strong authentication

Windows Hello

Microsoft Authenticator



FIDO2 Security Keys



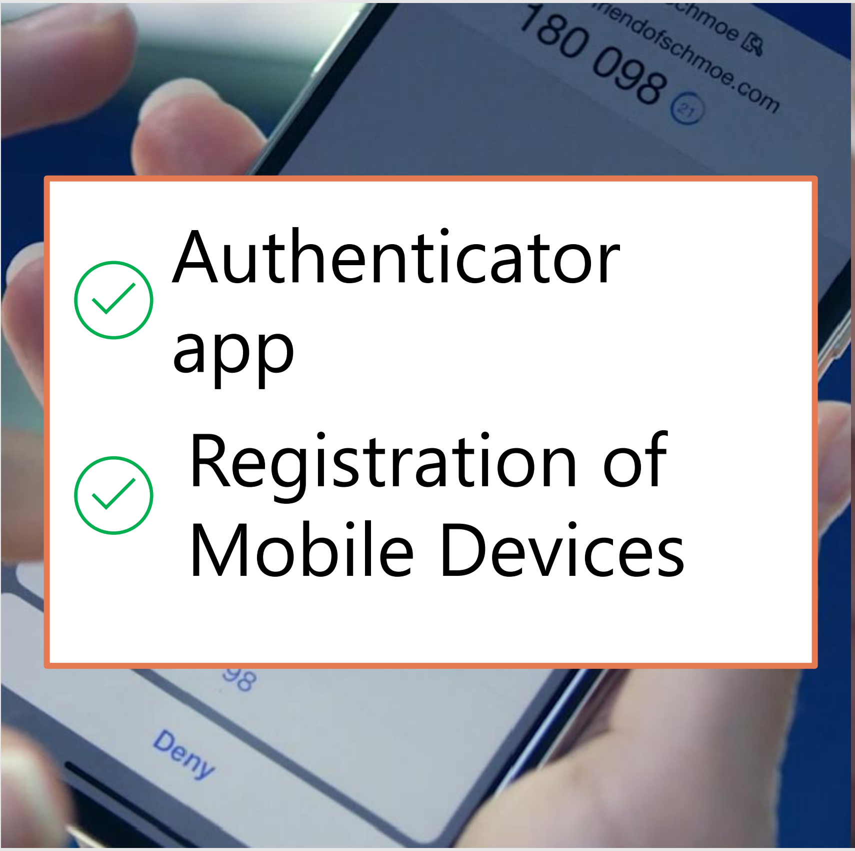
Power up your credentials

Passwordless foundation

Windows Hello

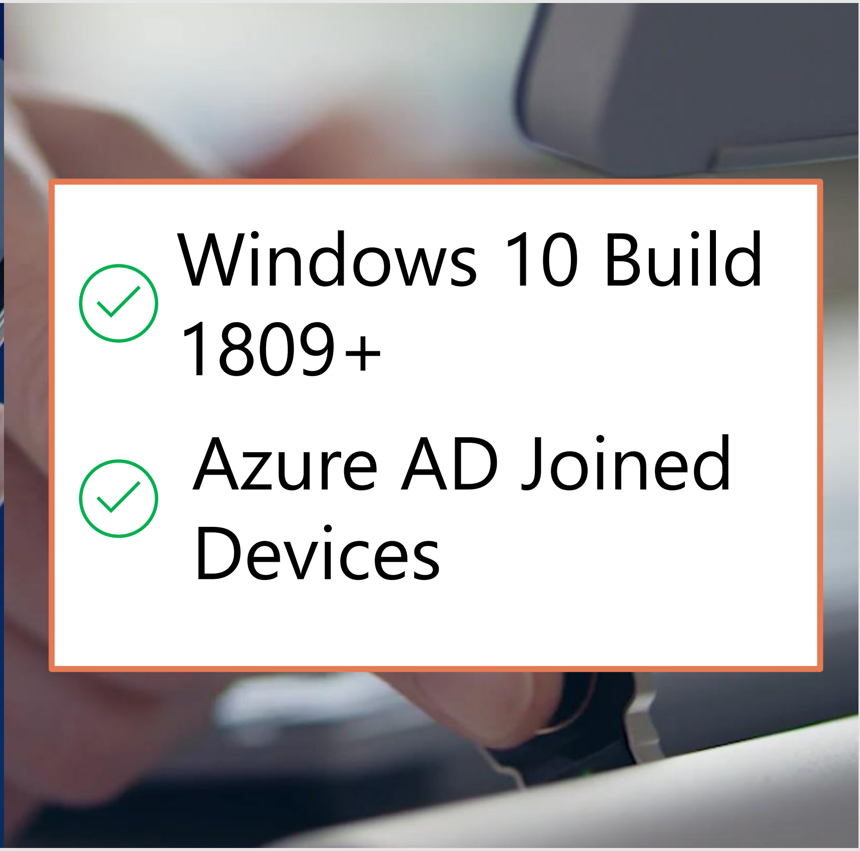
- ✓ Strong Credentials
- ✓ Registration of Windows Devices

Microsoft Authenticator



- ✓ Authenticator app
- ✓ Registration of Mobile Devices

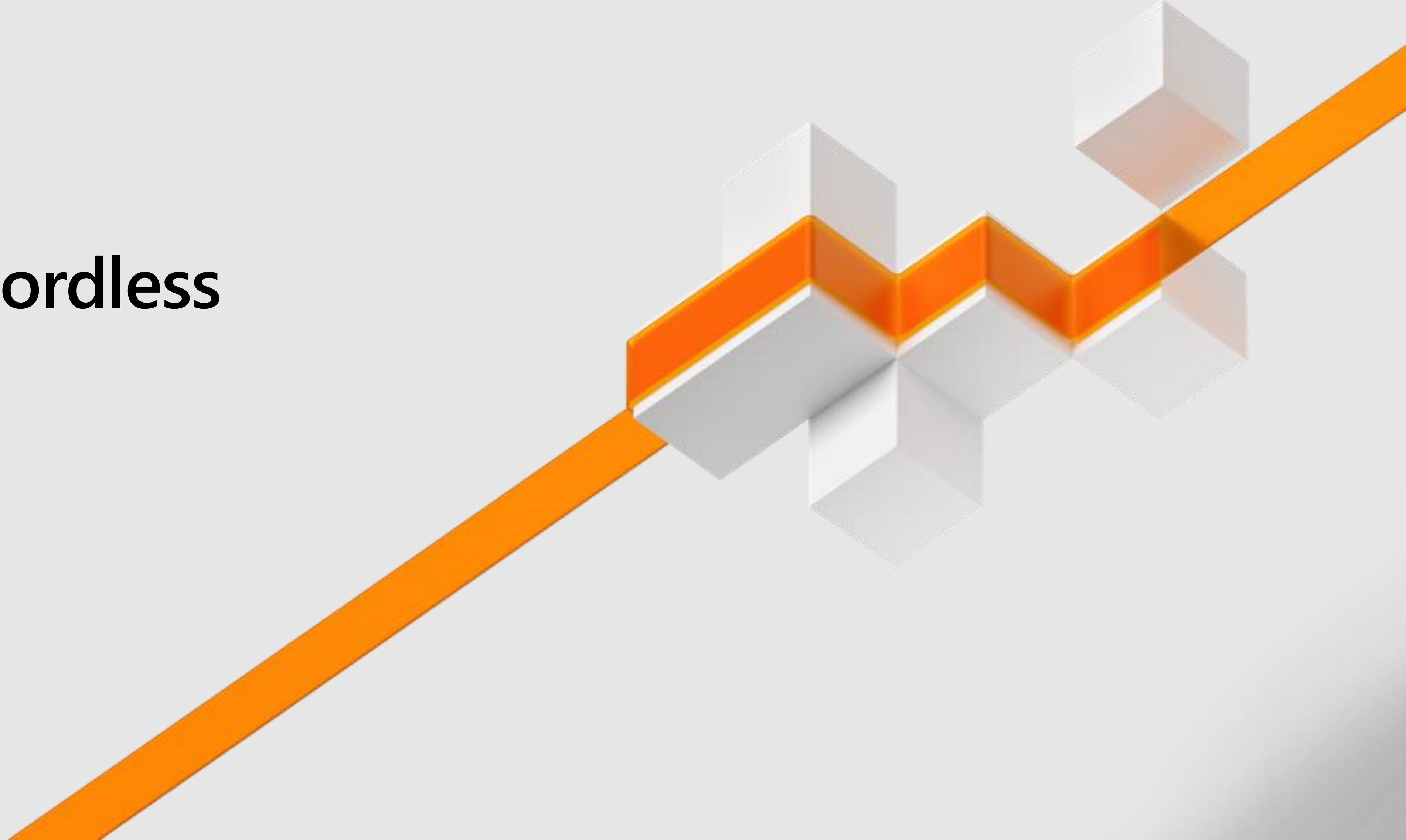
FIDO2 Security Keys



- ✓ Windows 10 Build 1809+
- ✓ Azure AD Joined Devices

Demo Passwordless

Get started quickly



Next steps -> Get the basics right

Strengthen your **credentials**

Multi-factor Auth (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 **security time to response** with better alerts

Enable **self-help** for predictable and integrated end user security

Microsoft

Move Beyond passwords – Securing your Microsoft 365 Tenant

Jan Ketil Skanke
MVP Enterprise Mobility
Principal Cloud Architect – CloudWay

Twitter @JankeSkanke

Microsoft