The background of the slide is a dark, monochromatic image of a mechanical safe. It features a large circular dial with numbers from 0 to 60, a metal handle, and several screws. The image is slightly blurred and has a dark, moody aesthetic.

Azure AD Identity protection



Arjan Cornelissen
SharePoint & Office 365 Architect
WorkTogether.tech
@arjancornelis

Work Together

SharePoint and office 365 Architect



Microsoft
CERTIFIED
Solutions Associate
Office 365

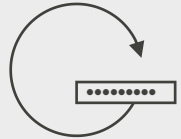
Microsoft
CERTIFIED
Solutions Expert
SharePoint

WORK TOGETHER

Azure AD Plans

	Free	O365 Apps	P1	P2
Identity and access management	500.000 objecten	Unlimited	Unlimited	Unlimited
SSO	10 apps	10 apps	Unlimited	Unlimited
Guest Users	X	X	X	X
Company branding		X	X	X
MFA		X	X	X
Self service password reset		X	X	X
Password Protection			X	X
Microsoft Cloud App Discovery			X	X
Azure AD Join			X	X
Dynamic groups			X	X
Conditional Access			X	X
Identity Protection				X
Identity Governance				X

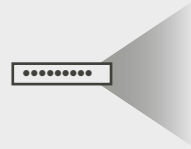
Top attacks against Azure AD



Breach
Replay

4.6B

attacker-driven sign-ins
detected in **May 2018**



Password
Spray

200K

password spray attacks
blocked in **August 2018**



Phishing

5B

high risk enterprise sign-in
attempts detected in **2018**



Passwords are the problem

WORK TOGETHER

Sobering statistics

140+



median # days attackers
reside **within** a victim's
network before
detection

75%+



network intrusions
due to compromised
user credentials

\$6T



annual cost
of cybercrime to the
global economy

\$4M



average cost of a
data breach to a
company

The frequency and sophistication of cybersecurity attacks are escalating

WORK TOGETHER

Updated NIST Guidelines

Three main changes:

1. No more periodic password changes
2. No more imposed password complexity
3. Validate new passwords against commonly used passwords

<http://aka.ms/passwordguidance>

Minimum Length Requirements (to defeat brute force hash attacks)

Don't use commonly attacked passwords

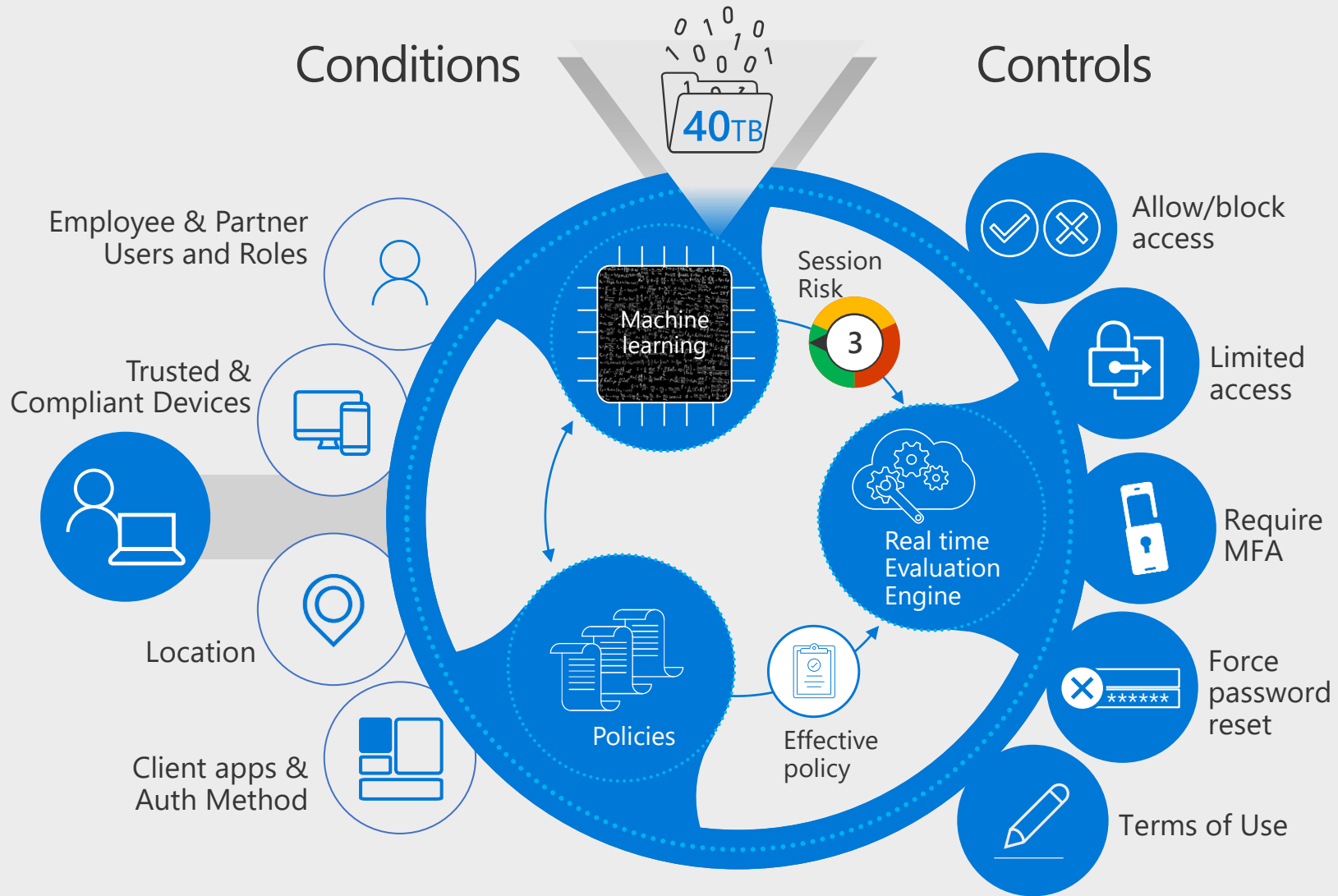
Use unique passwords

- Azure AD
- ADFS
- MSA
- Google ID

- Android
- iOS
- MacOS
- Windows
- Windows Defender ATP

- Geo-location
- Corporate Network

- Browser apps
- Client apps



Microsoft Cloud

Microsoft Cloud App Security



Cloud SaaS apps



On-premises apps

WORK TOGETHER



Demo Conditional Acces

Conditional Access

Intranet MFA policy with Duo

Info

Delete

* Name

Intranet MFA policy with Duo

Assignments

Users and groups

All users

Cloud apps

1 app included

Conditions

2 conditions selected

Access controls

Grant

1 control selected

Session

0 controls selected

Enable policy

On

Off

Grant

Select the controls to be enforced.

Block access

Grant access

☐ Require multi-factor authentication

☐ Require device to be marked as compliant

☐ Require domain joined (Hybrid Azure AD)

☐ Require approved client app (preview)

[See list of approved client apps](#)

☐ Employee TOU

☒ RequireDuoMfa

☐ Require RSA

☐ Trusona Mfa

For multiple controls

☐ Require all the selected controls

☒ Require one of the selected controls (preview)

Block legacy authentication

Info

Delete

* Name

Block legacy authentication

Assignments

Users and groups

All users included and specific us...

Cloud apps

All cloud apps

Conditions

1 condition selected

Access controls

Grant

Block access

Session

0 controls selected

Enable policy

On

Off

Conditions

Info

Sign-in risk

Not configured

Device platforms

Not configured

Locations

Not configured

Client apps (preview)

1 included

Device state (preview)

Not configured

Client apps (preview)

Configure

Yes

No

Select the client apps this policy will apply to

☐ Browser

☒ Mobile apps and desktop clients

☐ Modern authentication clients

☐ Exchange ActiveSync clients

☒ Other clients

WORK TOGETHER

Company Branding

21:34

<https://login.microsoftonline.com/>

Work Together
SharePoint and Office 365 Architect

arjan@worktogether.tech

Enter password

Because you're accessing sensitive info, you need to verify your password.

Password

[Forgot my password](#)

[Sign in with another account](#)

[Sign in](#)

Welcome at the sign in page of Work Together

©2018 Microsoft [Terms of use](#) [Privacy & cookies](#) ...

This site uses cookies for analytics, personalized content and ads. By continuing to browse this site, you agree to this use. [Learn more](#)

Work Together
SharePoint and Office 365 Architect

← arjan@worktogether.tech

Approve sign in

Tap the number you see below in your Microsoft Authenticator app to sign in.

80

[Use your password instead](#)

© 2018 Microsoft [Terms of use](#) [Privacy & cookies](#) ...

WORK TOGETHER



Demo Company
Branding |

Password protection

Home > Arjan Cornelissen > Authentication methods - Password protection

Authentication methods - Password protection

Arjan Cornelissen - Azure AD Security

Search (Ctrl+/) « Save Discard

Manage

- Authentication method policy (...)
- Password protection**

Custom smart logout

Lockout threshold ⓘ 10

Lockout duration in seconds ⓘ 60

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ

Password protection for Windows Server Active Directory

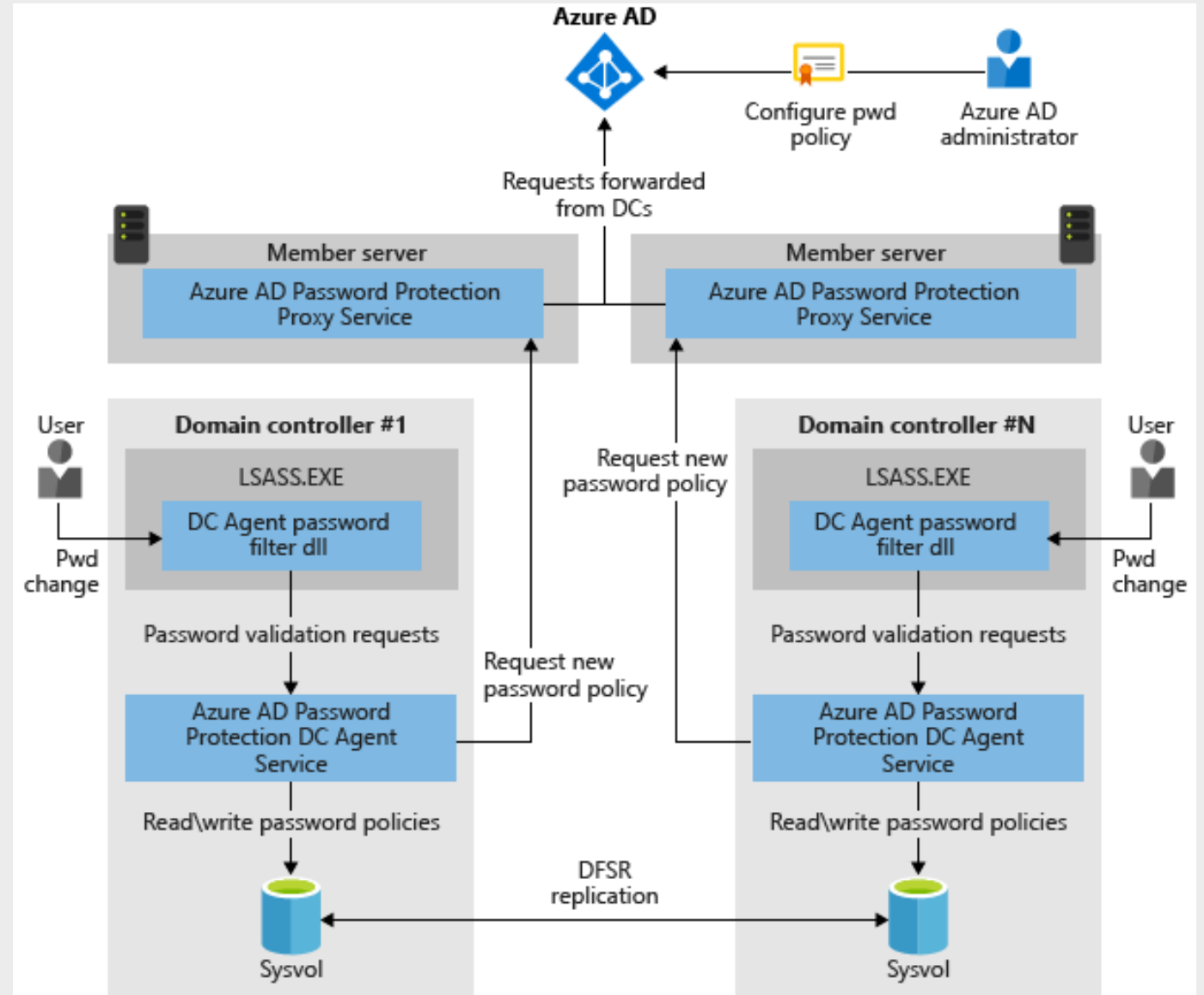
Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit



Demo Password Protection

Hybrid Password Protection

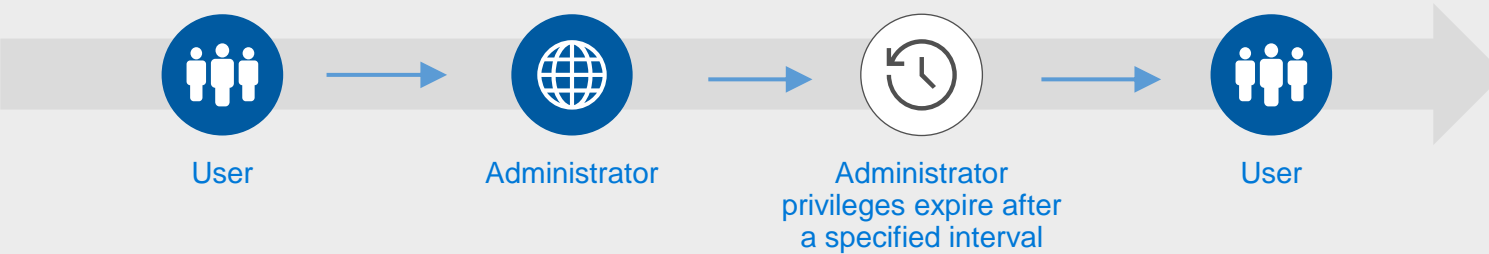


WORK TOGETHER

Admin side

Privileged Identity Management

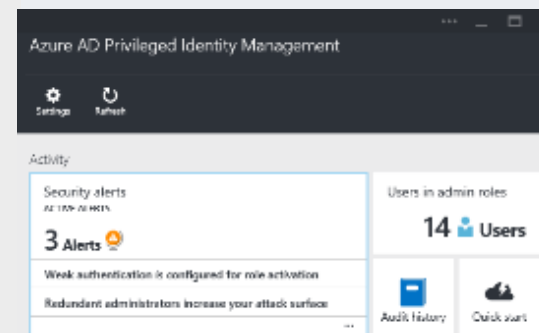
Discover, restrict, and monitor privileged identities



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 in Azure RBAC



WORK TOGETHER

Azure AD: Your privileged role was activated



Microsoft Azure <azure-noreply@microsoft.cor>

To Arjan Cornelissen

do 15-11-2018 08:34

[Reply](#) [Reply All](#) [Forward](#) [...](#)

[If there are problems with how this message is displayed, click here to view it in a web browser.](#)



Your Global Administrator role was activated in the WorkTogether.onmicrosoft.com directory

Activation details

Settings	Value
Expiration:	until 11/15/2018 9:34:06 AM UTC
Justification:	Session O365 Connect

You can re-activate or cancel your role activation in the [Azure Active Directory Privileged Identity Management extension](#) on the Azure portal.

[Learn more about Azure AD Privileged Identity Management >](#)

Work Together

Arjan Cornelissen (private O365) is now eligible to activate the Reader role for Visual Studio Enterprise – MPN subscription

The details of this assignment appear below.

View the details of this assignment in the Privileged Identity Management (PIM) portal.

[View details >](#)

Settings	Value
User or Group	Arjan Cornelissen (private O365)
Role	Reader
Resource name	Visual Studio Enterprise – MPN
Resource type	subscription
Updated by	Arjan Cornelissen
Assignment type	Eligible
Assignment start	December 12, 2018 22:02 UTC
Assignment end	March 12, 2019 22:02 UTC
Justification	-

[Privileged Identity Management](#) protects your organization from accidental or malicious activity by reducing persistent access to Azure resources, providing just-in-time or time-limited access when needed.

Privileged Identity

WORK TOGETHER

Roles

Work Together

Default for all roles

Application Administrator

Application Developer

Billing Administrator

Cloud Application Administrator

Cloud Device Administrator

Compliance Administrator

Conditional Access Administrator

CRM Service Administrator

Customer LockBox Access Approver

Desktop Analytics Administrator

Device Administrators

Directory Readers

Directory Writers

Exchange Administrator

Global Administrator

Guest Inviter

Information Protection Administrator

Intune Service Administrator

License Administrator

Message Center Reader

Password Administrator

...

Global Administrator

Save Discard

Activations

Maximum activation duration (hours) ⓘ

2

Notifications

Send email notifying admins of activation ⓘ

Enable Disable

Incident/Request ticket

Require incident/request ticket number during activation ⓘ

Enable Disable

Multi-Factor Authentication

Require Azure Multi-Factor Authentication for activation ⓘ

Enable Disable

Require approval

Require approval to activate this role ⓘ

Enable Disable

Identity Secure Score

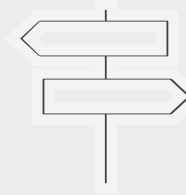
Visibility into your Identity security position and how to improve it



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.

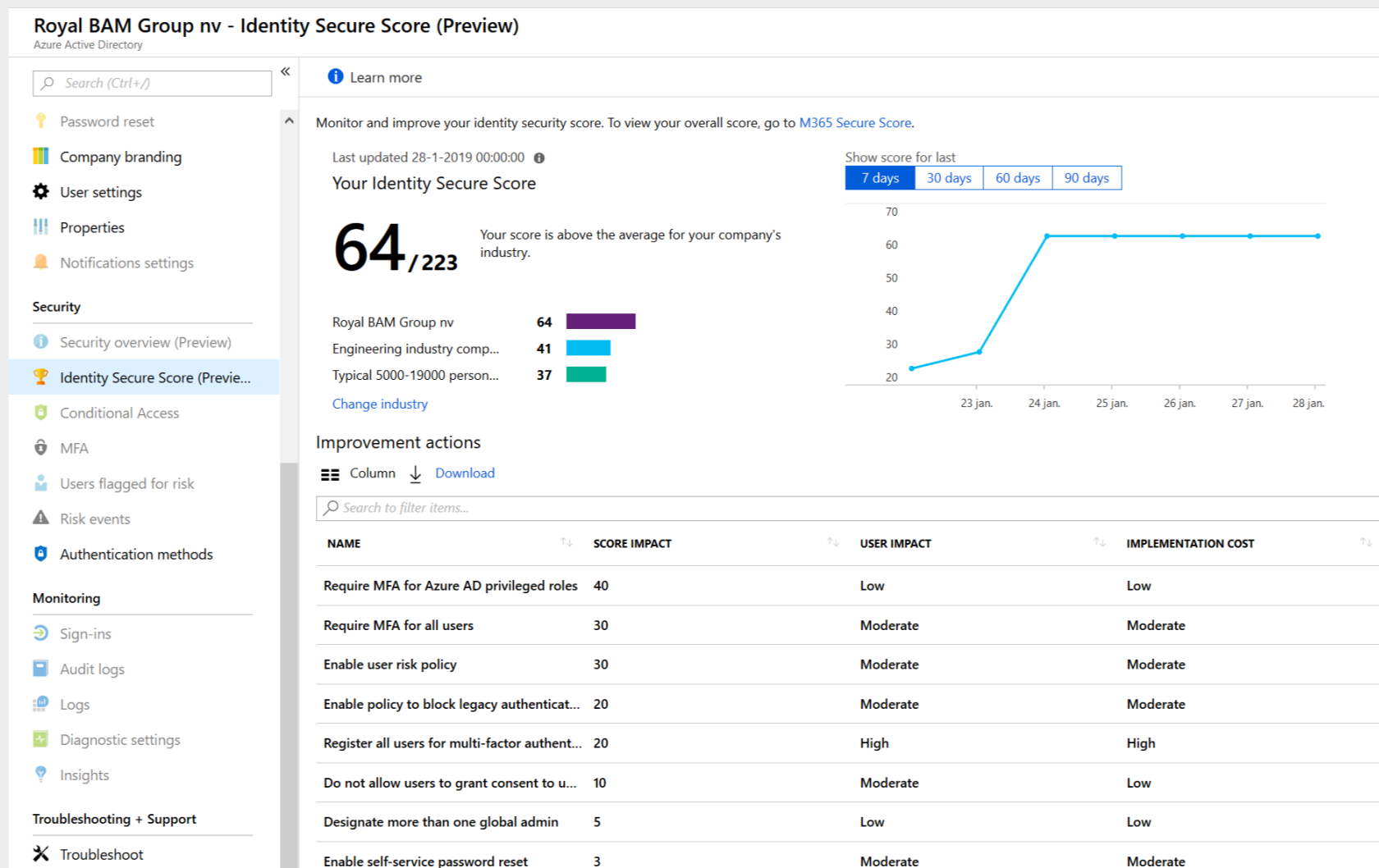
- Ignore controls that are not valid for you.

- 3rd party product support.

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

WORK TOGETHER

Secure Score



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

WORK TOGETHER

Preview features



Password-less with Microsoft Authenticator app

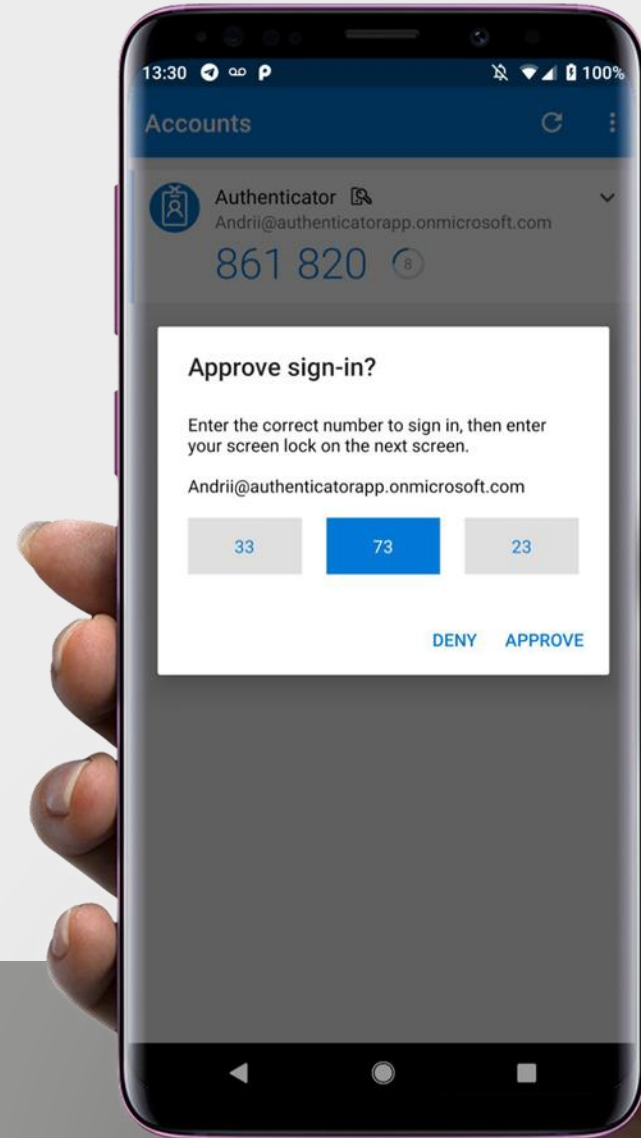
Password-less for MSA accounts

Available today

Password-less for Azure AD accounts

In Public preview today

aka.ms/gopasswordless





Demo Password less authentication

Getting the basics right



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](#))

Our Security mindset
needs to be updated