Microsoft

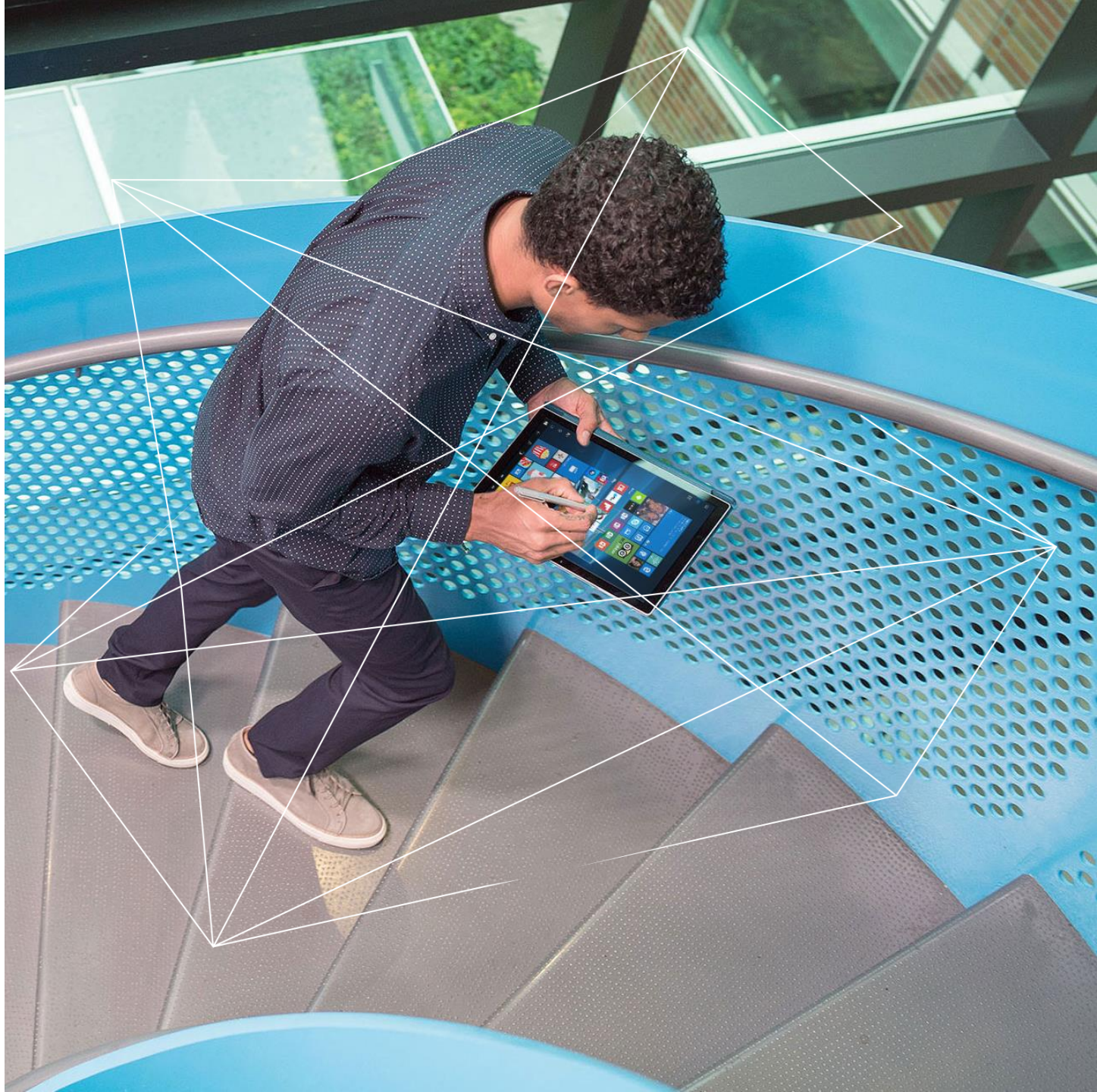
Protecting identities by using Azure Active Directory

Damir Dizdarević
Logosoft d.o.o. Sarajevo
ddamir@logosoft.ba

MVP Microsoft® Most Valuable Professional

Microsoft® Regional Director

#ntk18



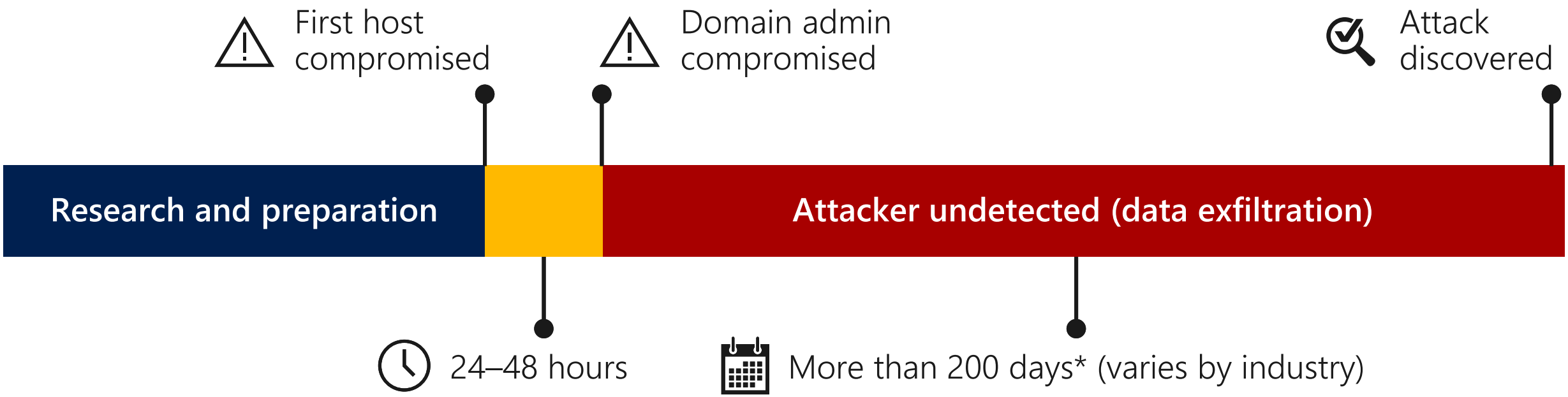
TURBULENT TIMES

300% increase in user account attacks this year

96% of malware is automated polymorphic

$15 MILLION of cost/business impact per breach

Attack timeline



Attack sophistication

Attack operators exploit any weakness

Target information on any device or service

Target AD and identities

Active Directory controls access to business assets

Attackers commonly target AD and IT Admins

Attacks not detected

Current detection tools miss most attacks

You may be under attack (or compromised)

Response and recovery

Response requires advanced expertise and tools

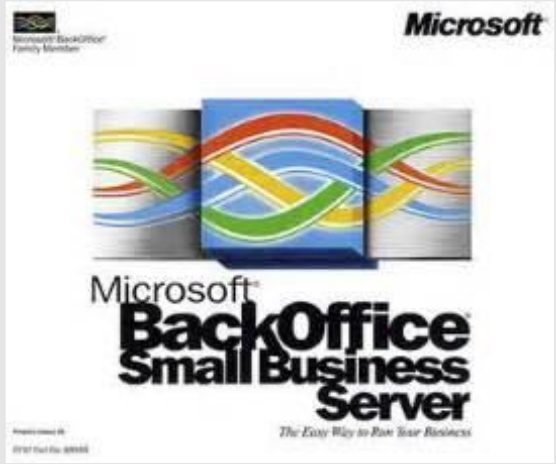
Expensive and challenging to successfully recover

So, what can we do to protect identites?

- Use stronger passwords?
- Change passwords more often?
- Use smart cards?
- Not exactly…

We go for a major change in identity store

For 20 years, Microsoft has recommended local Active Directory Domain Services for businesses with more than 10 users.



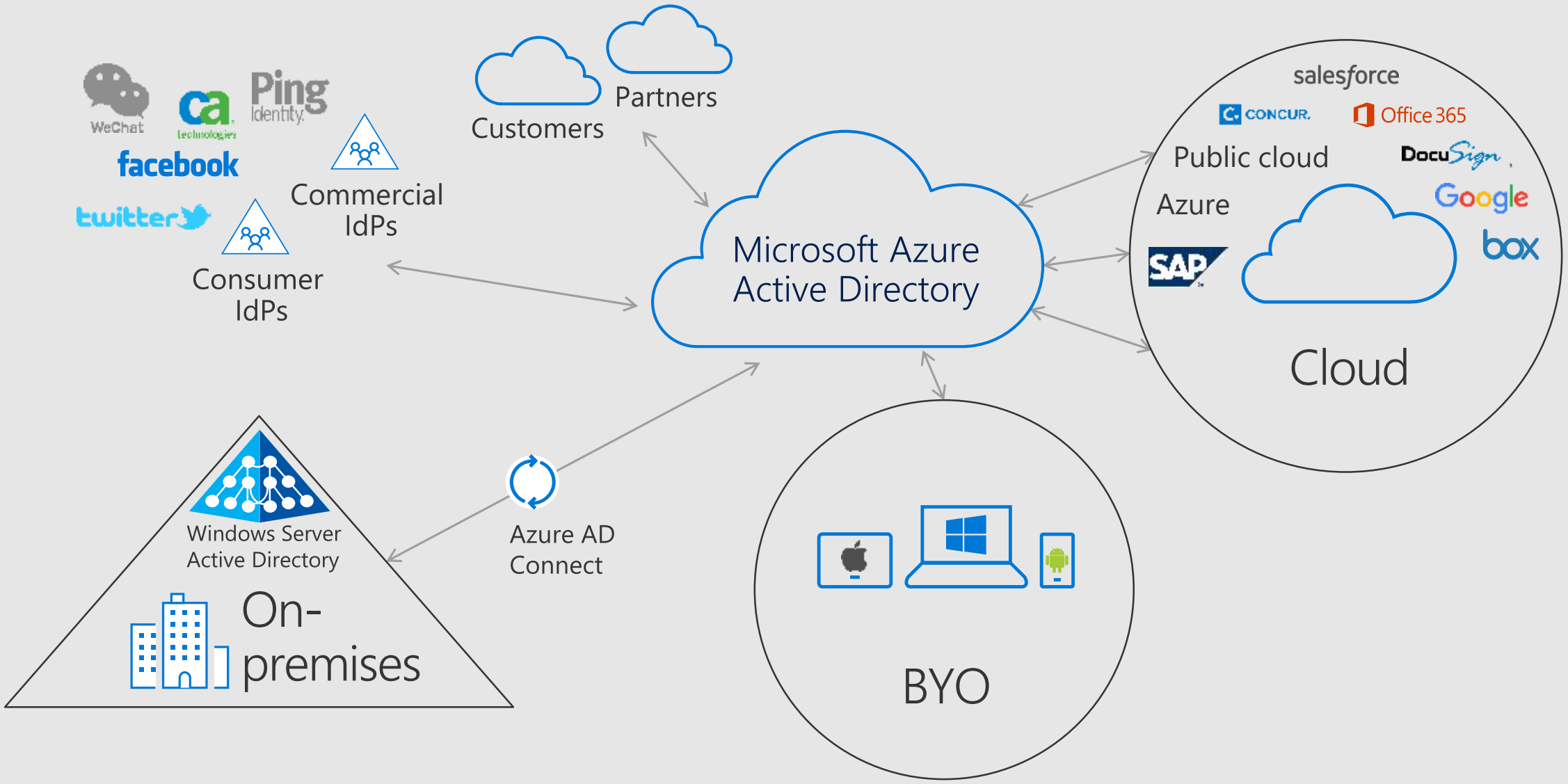
Yesterday

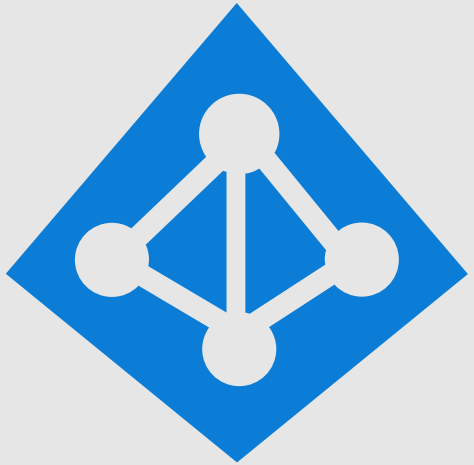
Change in identity

Now we have a new way to think.

Today

Azure AD - Identity as the Control Plane



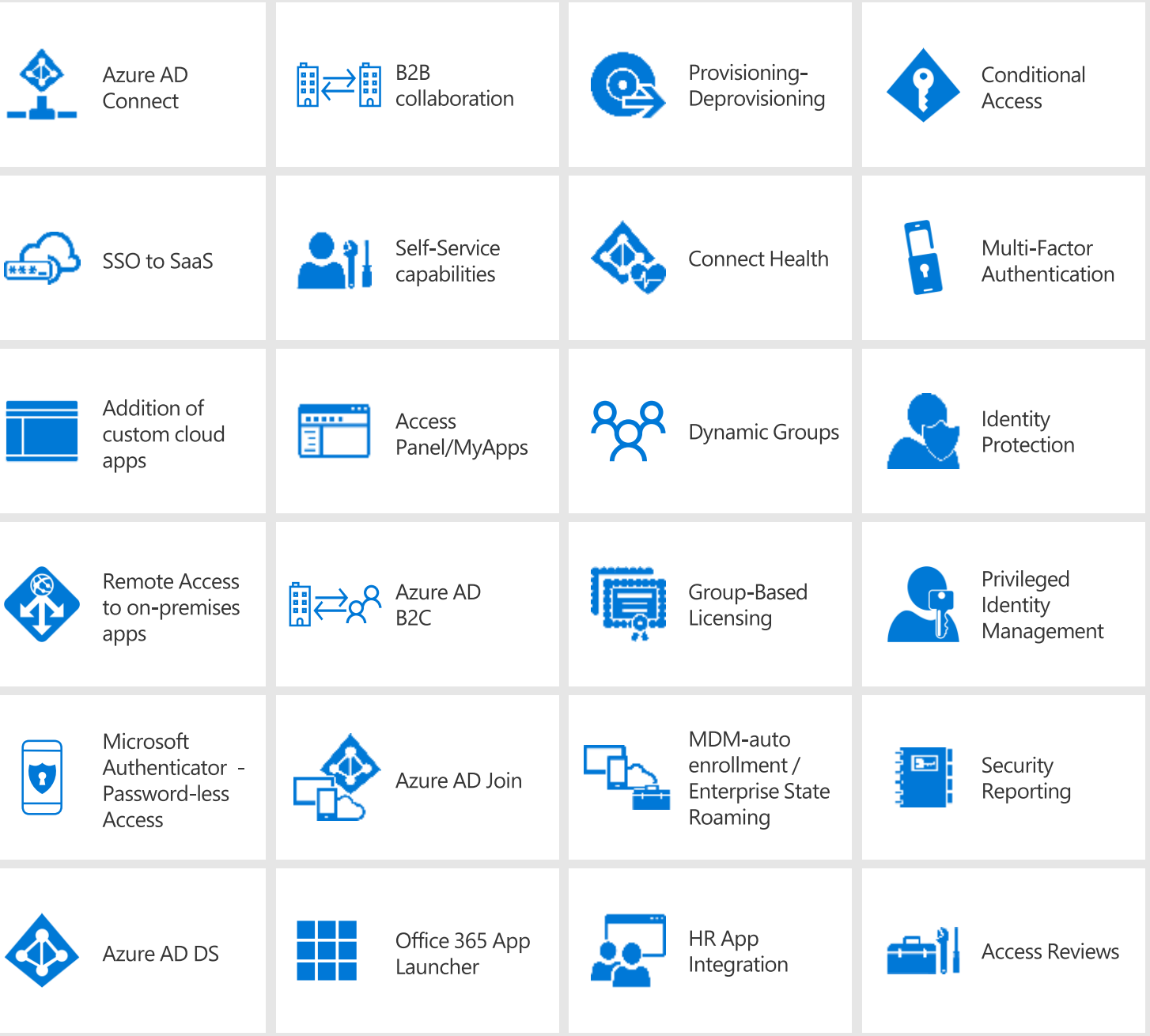


Azure Active Directory

Azure AD Connect	B2B collaboration	Provisioning- Deprovisioning	**Conditional Access**
SSO to SaaS	**Self-Service capabilities**	Connect Health	**Multi-Factor Authentication**
Addition of custom cloud apps	Access Panel/MyApps	Dynamic Groups	**Identity Protection**
Remote Access to on-premises apps	Azure AD B2C	Group-Based Licensing	**Privileged Identity Management**
Microsoft Authenticator - Password-less Access	Azure AD Join	MDM-auto enrollment / Enterprise State Roaming	Security Reporting
Azure AD DS	Office 365 App Launcher	HR App Integration	**Access Reviews**

Identity and Access Management Use Cases

1. I want to provide my employees **secure and easy access to every application** from any location and any device
2. I want to **quickly deploy applications** to devices, do more with less and automate Join/Move/Leave processes
3. I need my customers and partners to **access the apps they need from everywhere** and collaborate seamlessly
4. I want to **protect access to my resources** from advanced threats
5. I need to **comply with industry regulation** and national data protection laws
6. I want to write applications that **work with my corporate identities in Azure Active Directory**



Benefits of moving to AAD

Have Office 365? Already have AAD

Office 365 — Office apps — Edge browser — Internet Explorer — Windows 10

Single identity

Single identity-management interface

Computer sign in — Office 365 — Microsoft Admin Center

Challenges and recommendations

User profiles
Manual Profile migration for existing machines

GPOs
No Management for GPOs

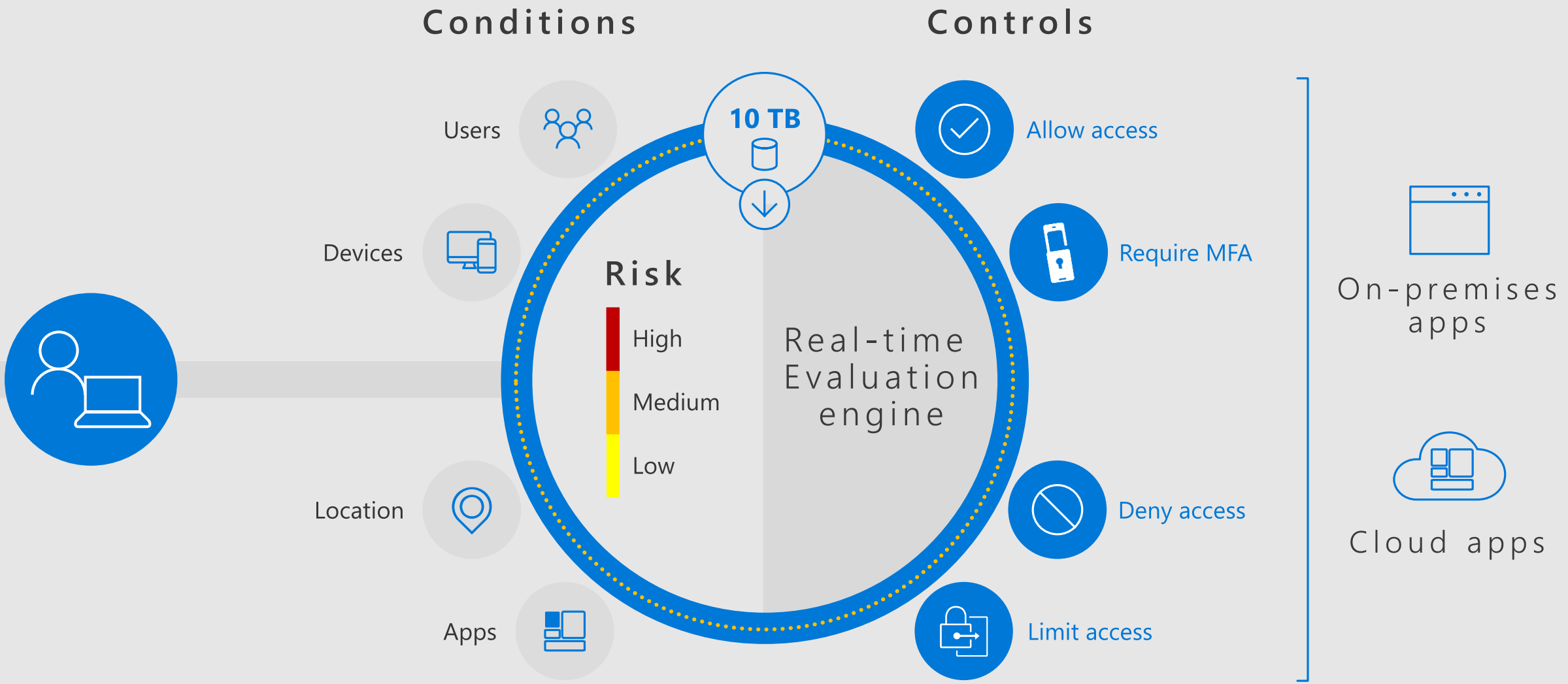
Local resources
Access to local resources during transition

AD connect
Password changes for on-premises resources

How do we protect identities in Azure AD?

- *Conditional access*
- *Azure MFA*
- *Windows Hello*
- *Passwordless approach*
- *Privileged Identity Protection*

CONDITIONAL ACCESS



Azure Multi-Factor Authentication

Strong and secure authentication for on-premises, hybrid & the cloud

- Available as Azure MFA service and Azure MFA Server (on-premises)
- App Passwords for users are needed for some non-browser apps that do not support MFA
- Always enable MFA for admins, preferrably also for users with conditional access
  - Whitelist known and trusted IP address spaces to bypass MFA

Windows Hello for Business

- User authentication to an AAD account
- PIN, biometric or gesture is verified locally with TPM
- The TPM holds the private key that never leaves the device.
- AAD holds the public key and verifies identity against the device held private key.

No passwords = more secure

Fast IDentity Online 2.0

Standards-based, interoperable authentication

Works with the same devices people use every day

Based on public key cryptography

Biometrics and keys never leave the device

Protects against phishing, man-in-the-middle and replay attacks

fido™ alliance 2.0

FIDO Alliance board members

...and hundreds of industry partners

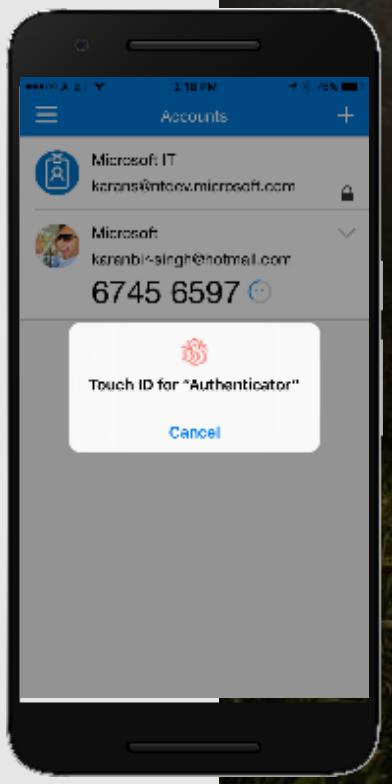
Microsoft Account

Phone sign-in using Microsoft Authenticator

Password-less authentication

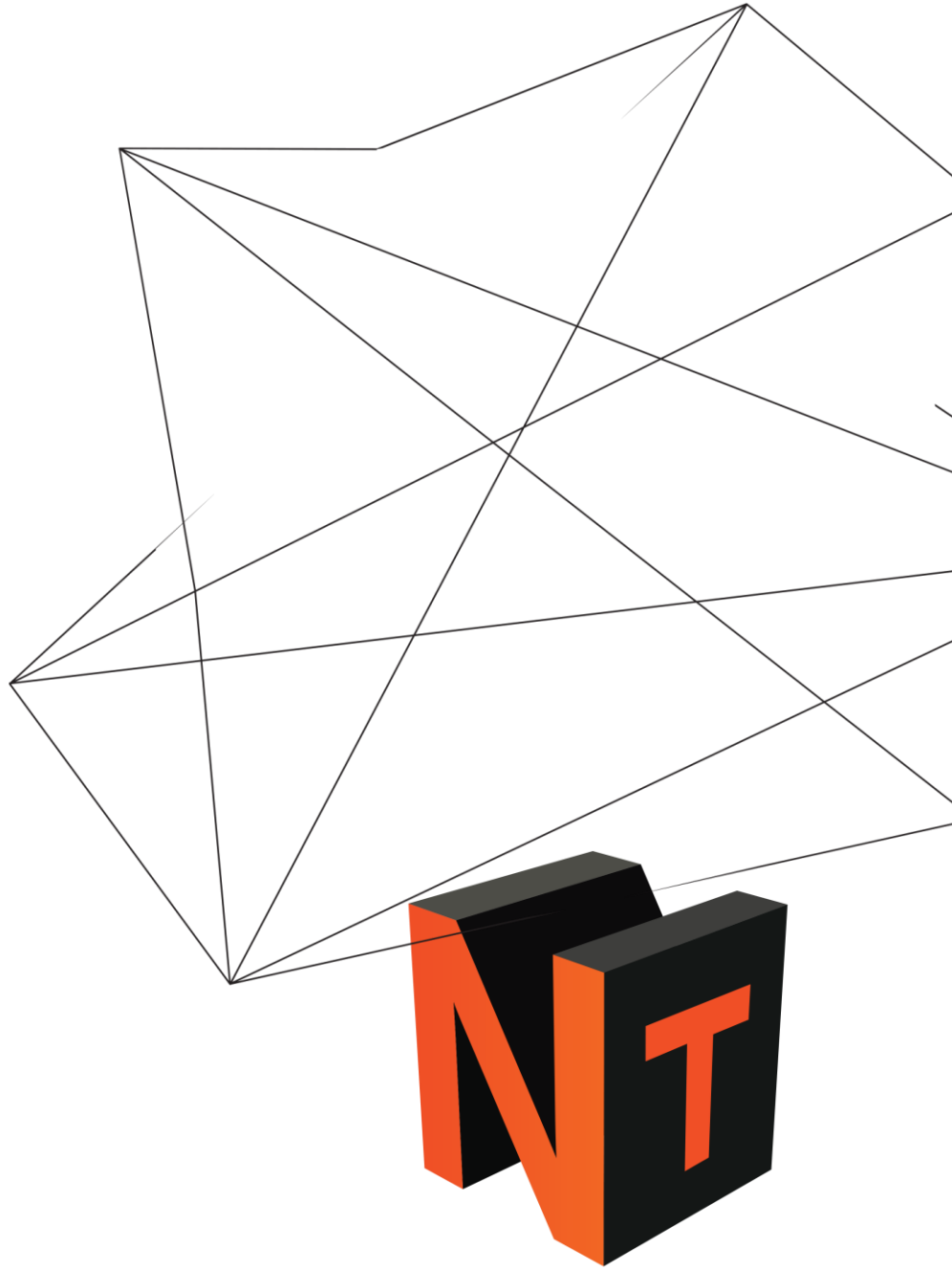
Public / Private key exchange

Available today!



Demo

Passwordless access for Microsoft account



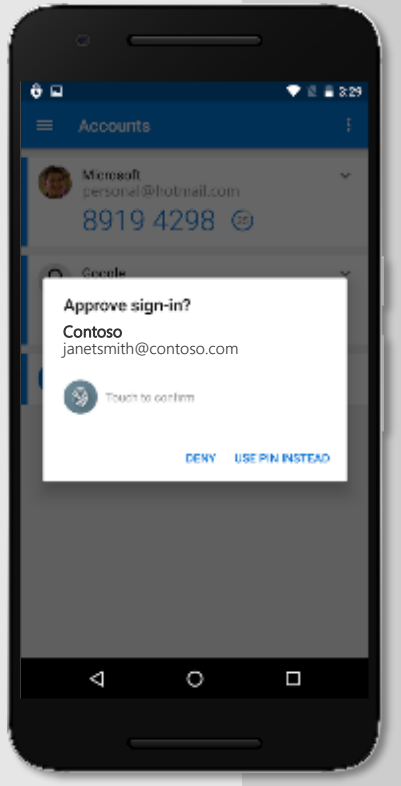
Azure Active Directory

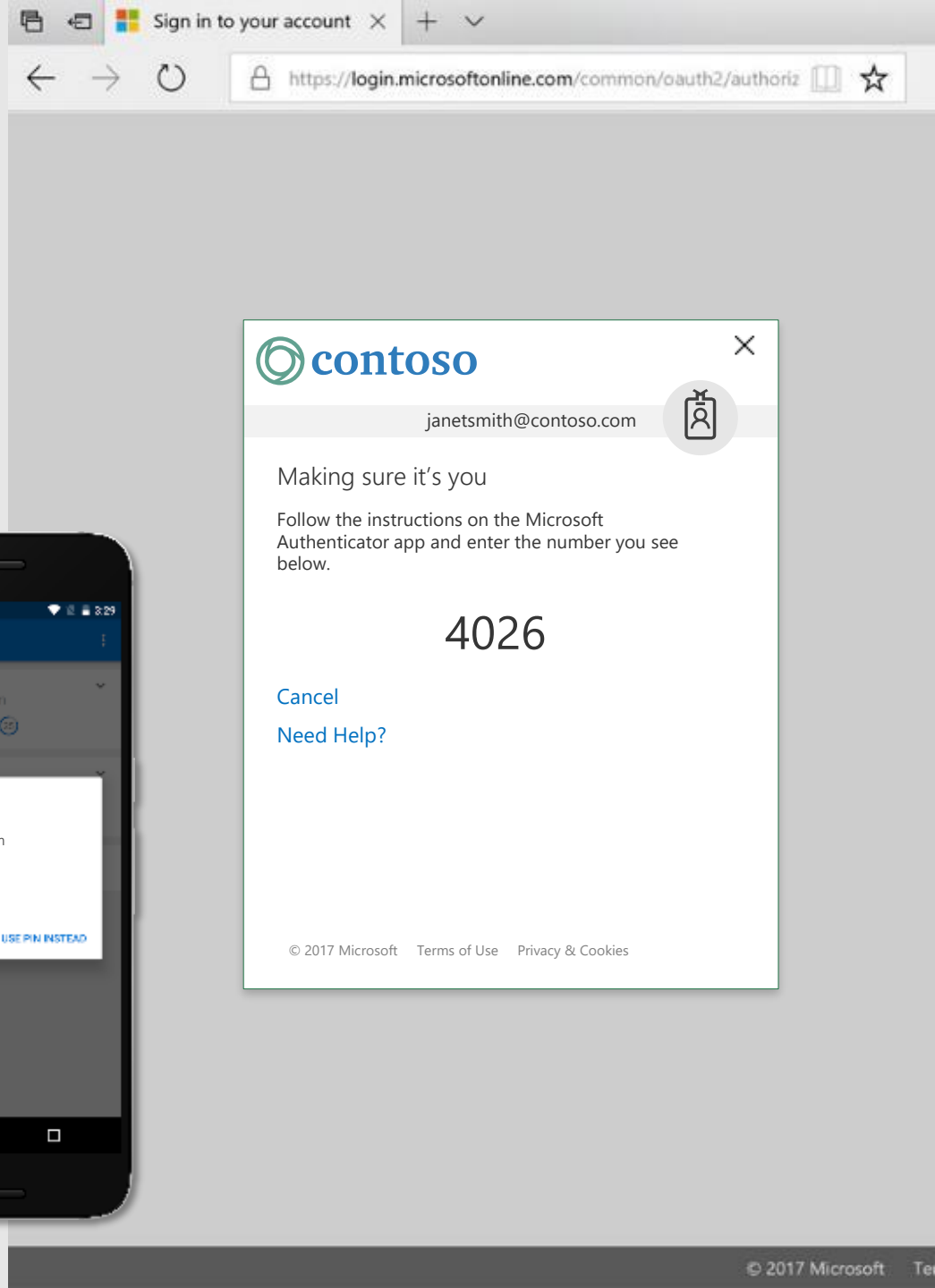
Phone sign-in using Microsoft Authenticator

Passwordless authentication

Public / Private key exchange

Coming in Spring/Summer 2018





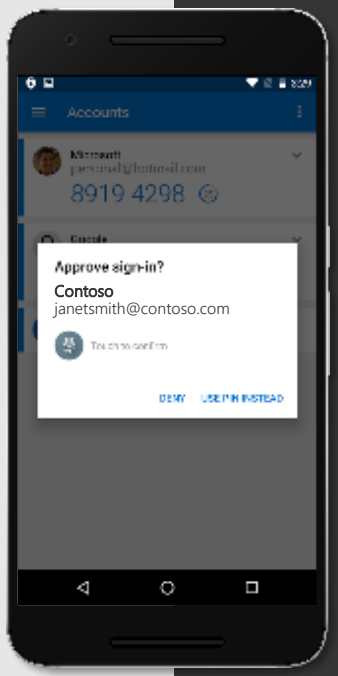
Microsoft Authenticator

+ fido™

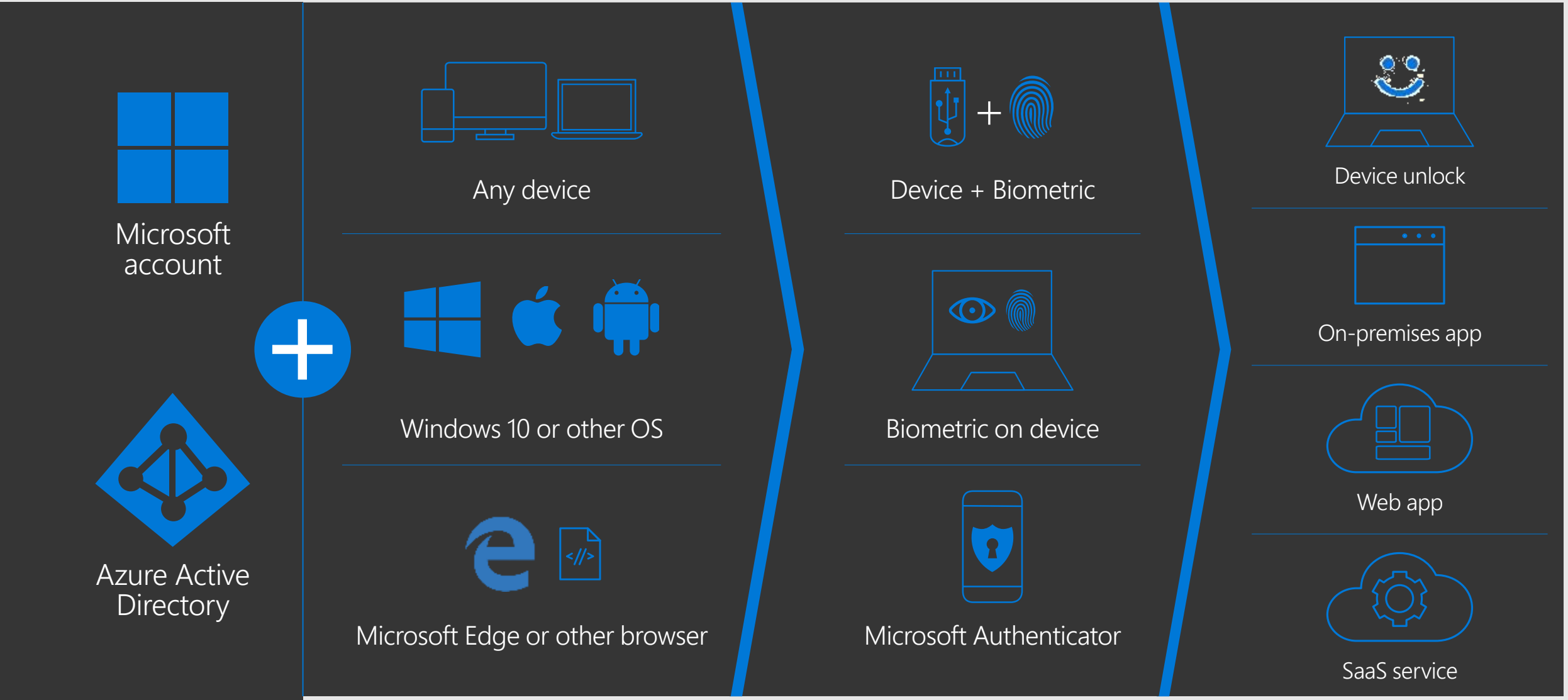
Add FIDO 2.0 support

Great solution for Windows 7, MacOS, and Linux

Coming in Summer 2018



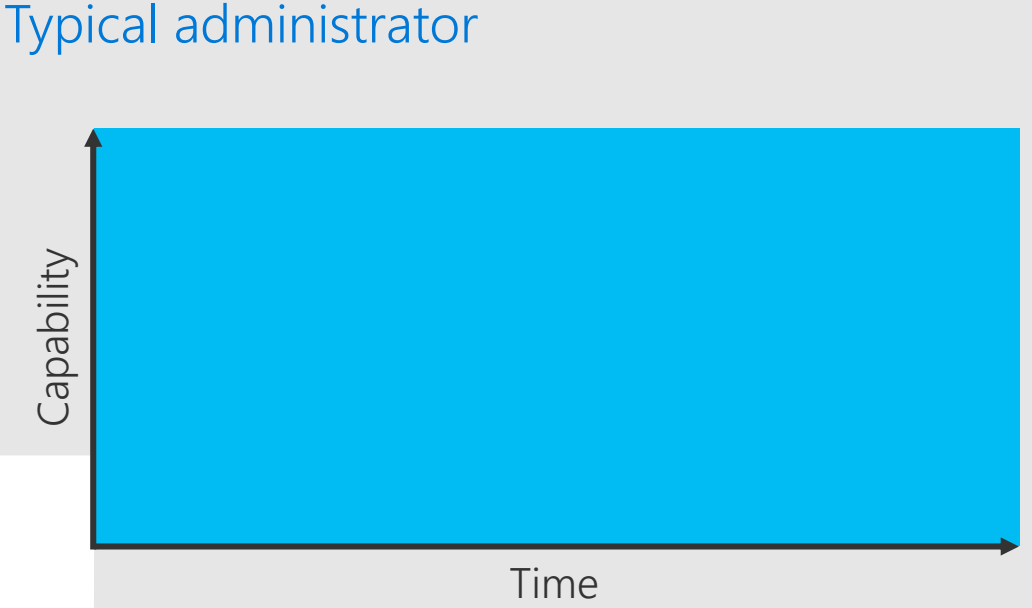
The roadmap to no more passwords



Challenges in protecting credentials

- Social engineering leads to credential theft.
- Most identity attacks remain undiscovered for 200+ days
- Most attacks seek out and leverage administrative credentials.

  Administrative credentials often inadvertently provide more privilege than necessary—and for an unlimited time.



Protect against compromised admin credentials

Credential Guard

Prevents Pass the Hash and Pass the Ticket attacks by protecting stored credentials through Virtualization based Security (VBS)

Remote Credential Guard

Works in conjunction with Credential Guard for RDP session providing SSO for RDP sessions while eliminating the need for credentials to be passed to the RDP host

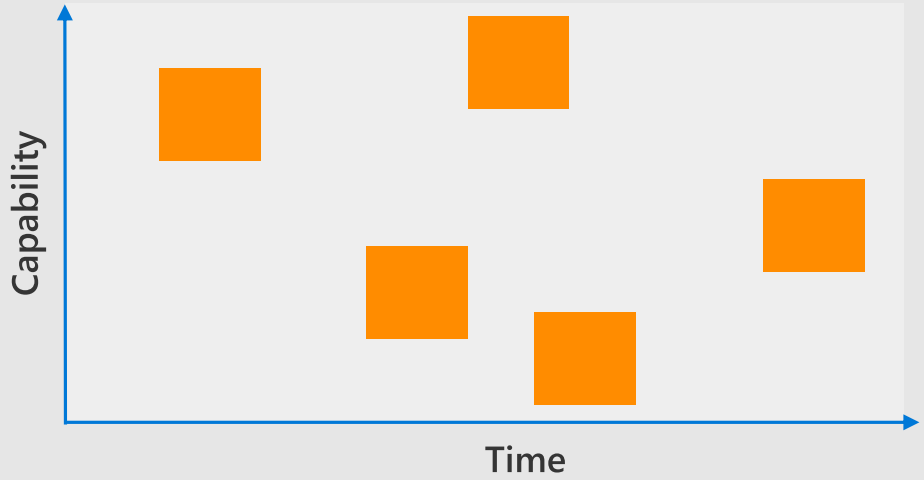
Just enough administration

Administration Limits administrative privileges to the bare-minimum required set of actions (limited in space)

Just-in-time administration

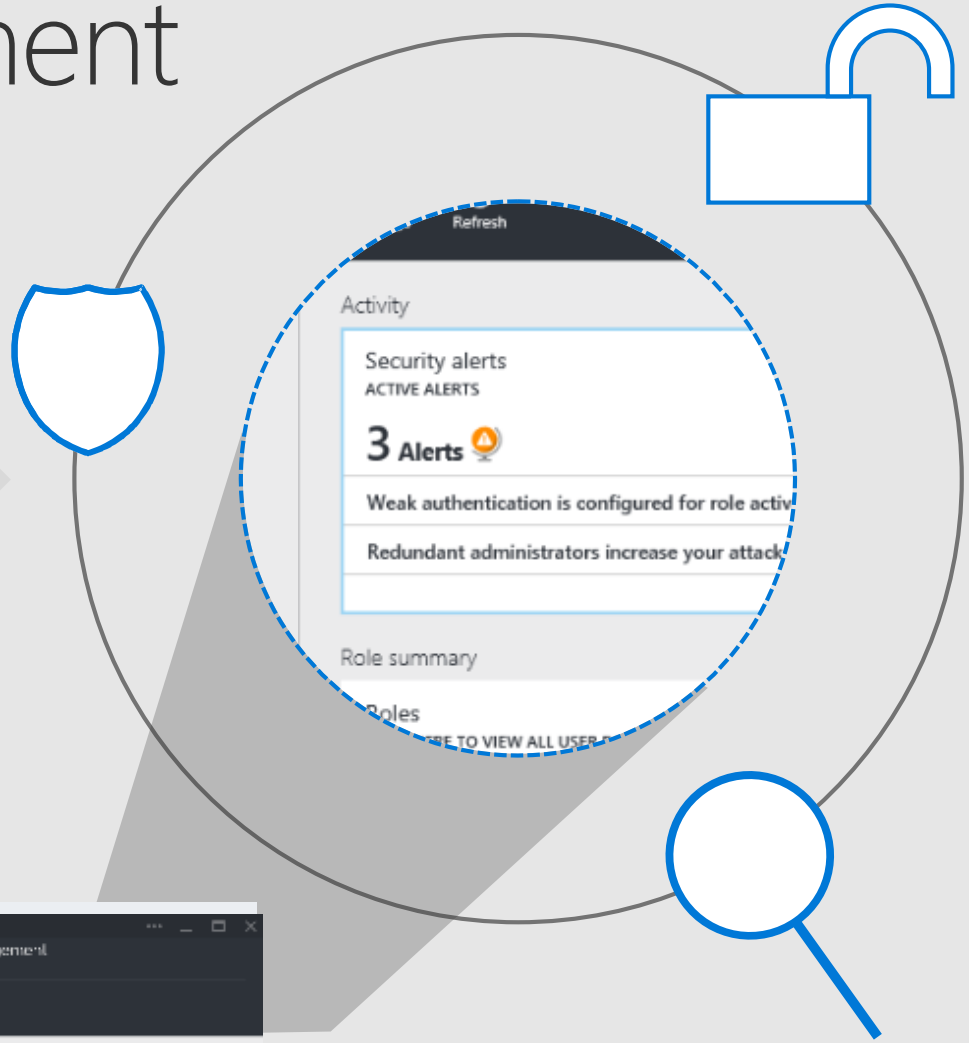
Administration Provide privileged access through a workflow that is audited and limited in time

Just enough and just-in-time administration



Privileged Identity Management

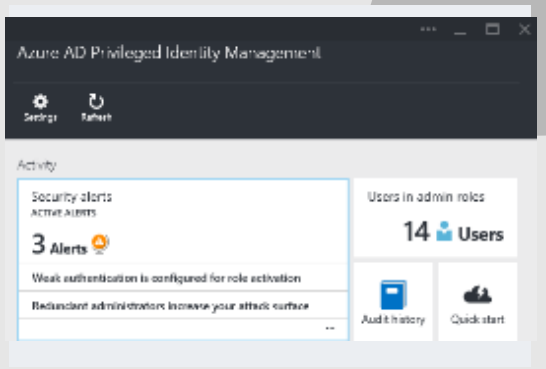
Discover, restrict, and monitor privileged identities



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

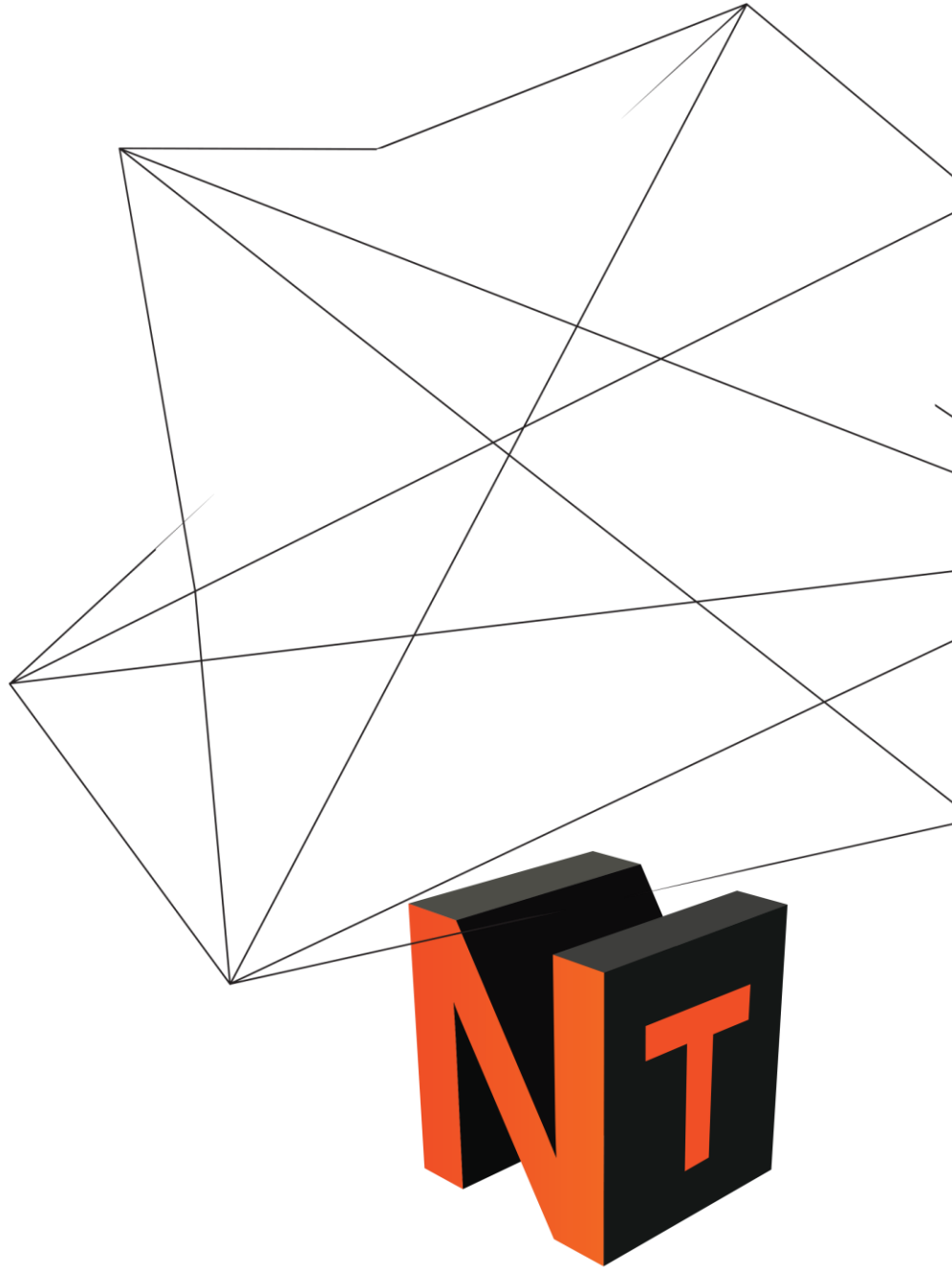
Ensure policies are met with alerts, audit reports and access reviews

Manage admins access in Azure AD and also in Azure RBAC

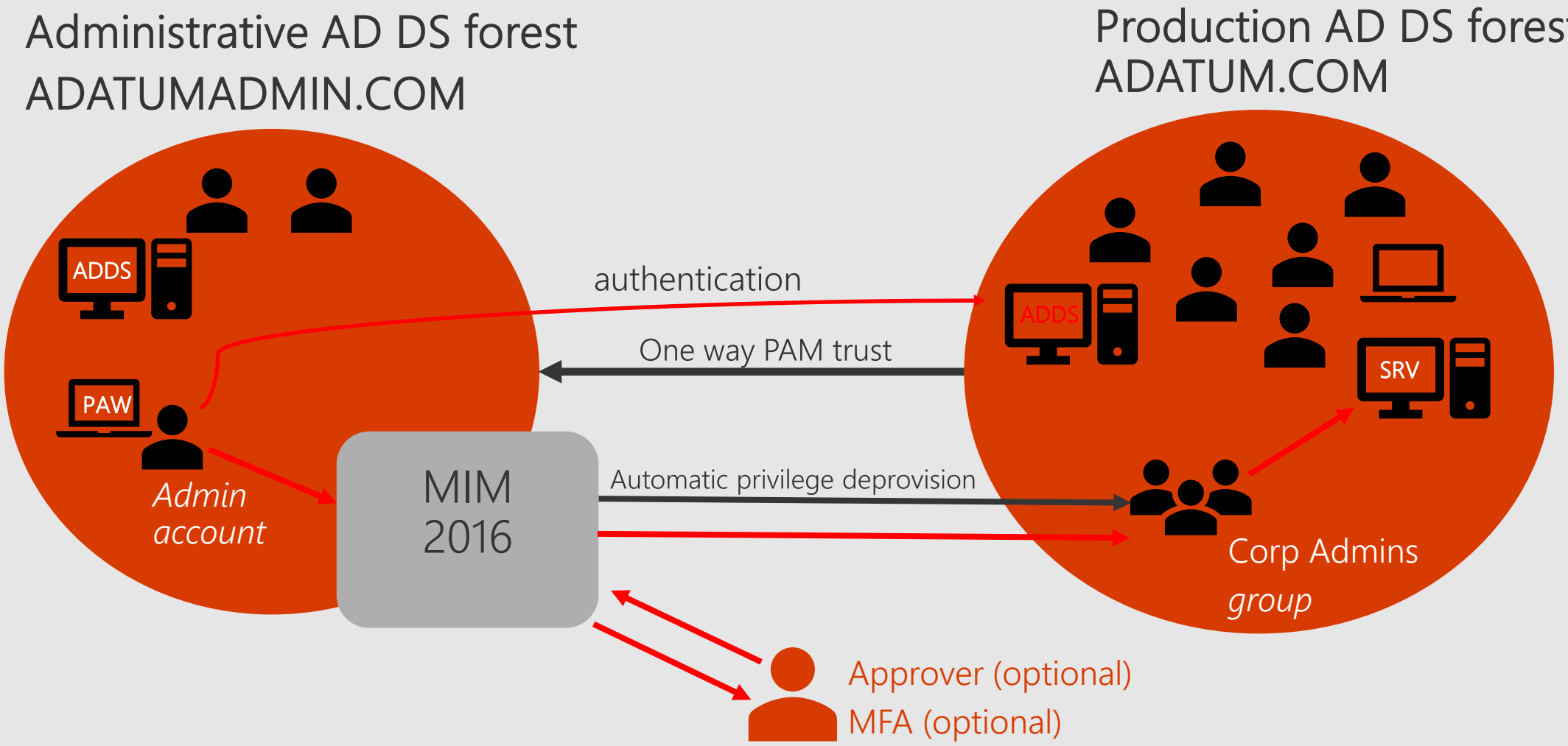


Demo

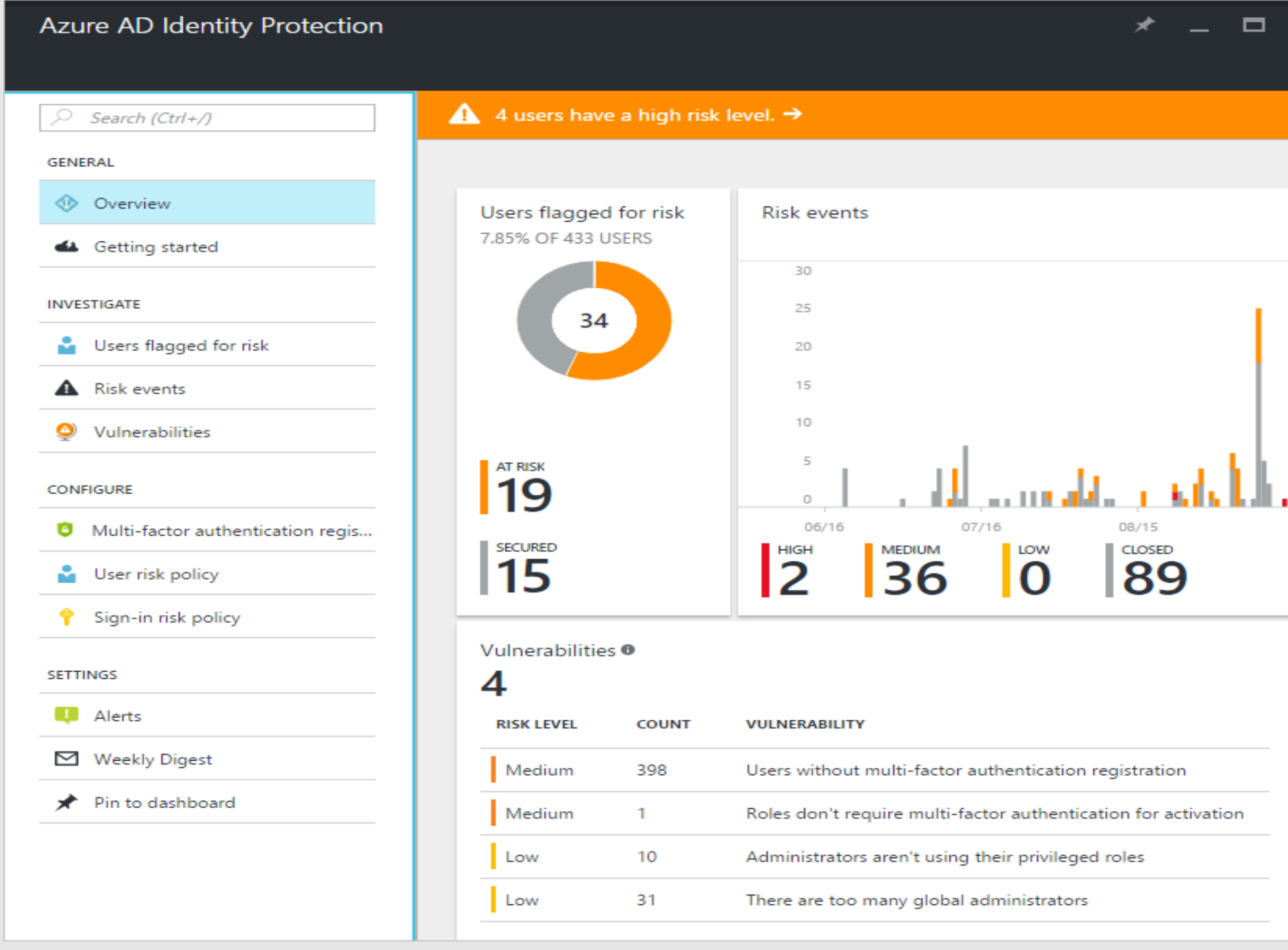
Privileged Identity Management in Azure AD



PIM on-premises

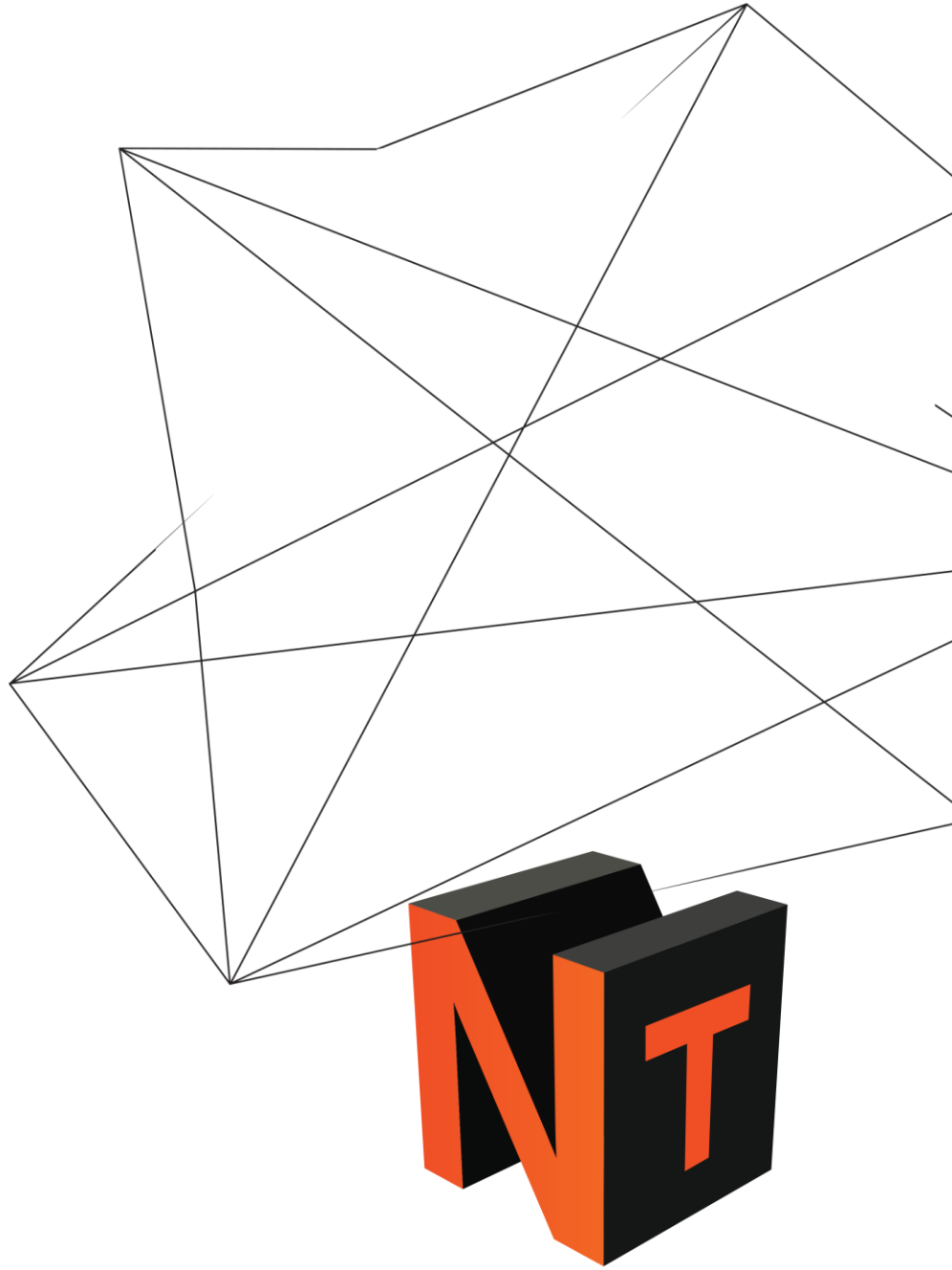


Azure AD Identity Protection



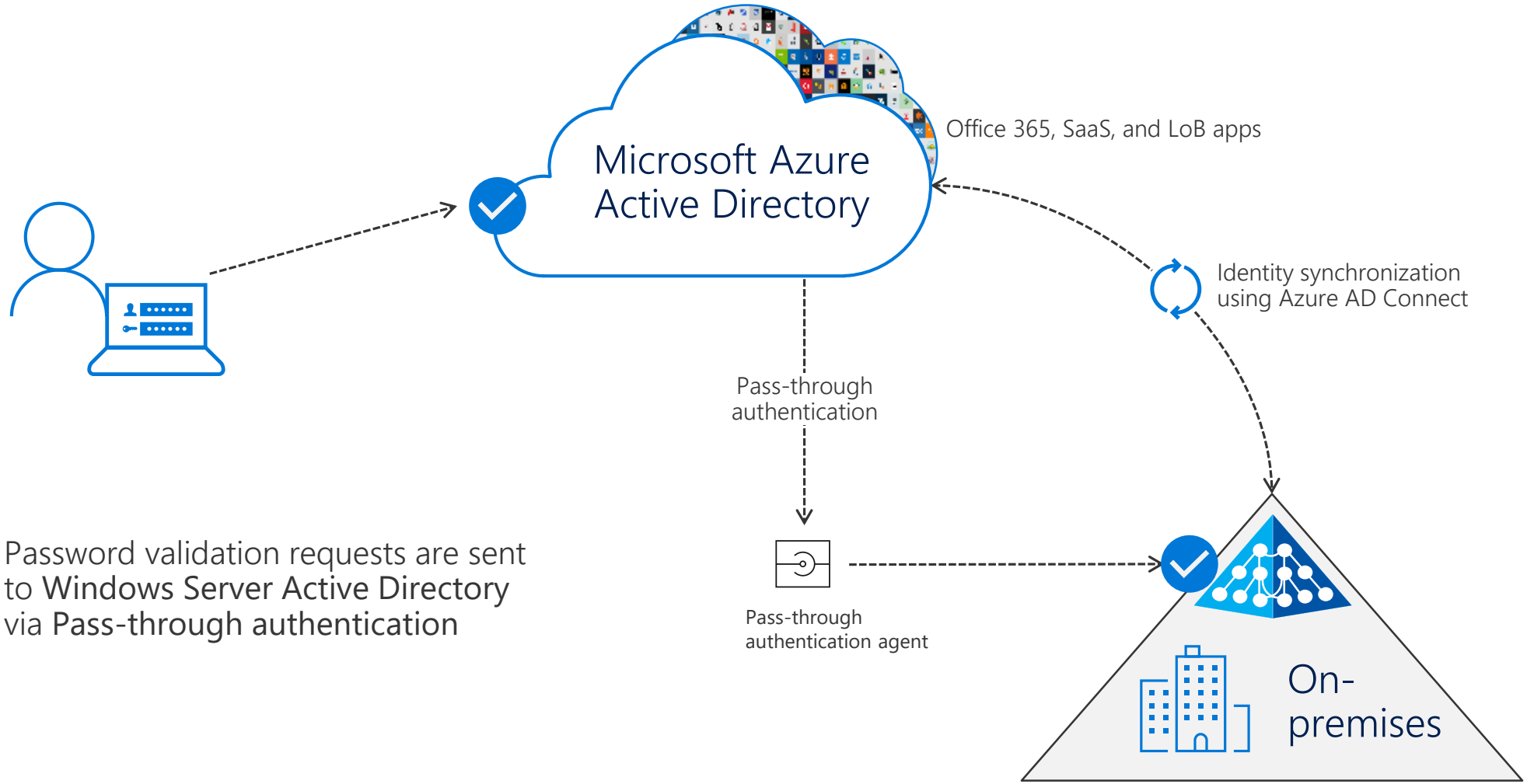
Demo

Identity Protection in Azure AD



Pass-through authentication is Generally Available

Identity synchronization + Pass-through authentication with Seamless SSO



Password validation requests are sent to **Windows Server Active Directory** via **Pass-through authentication**

Thanks for your attention!

Feel free to ask: ddamir@logosoft.ba