Wiki Webinar

by inetum. realdolmen

Identity Protection: meer dan enkel een wachtwoord

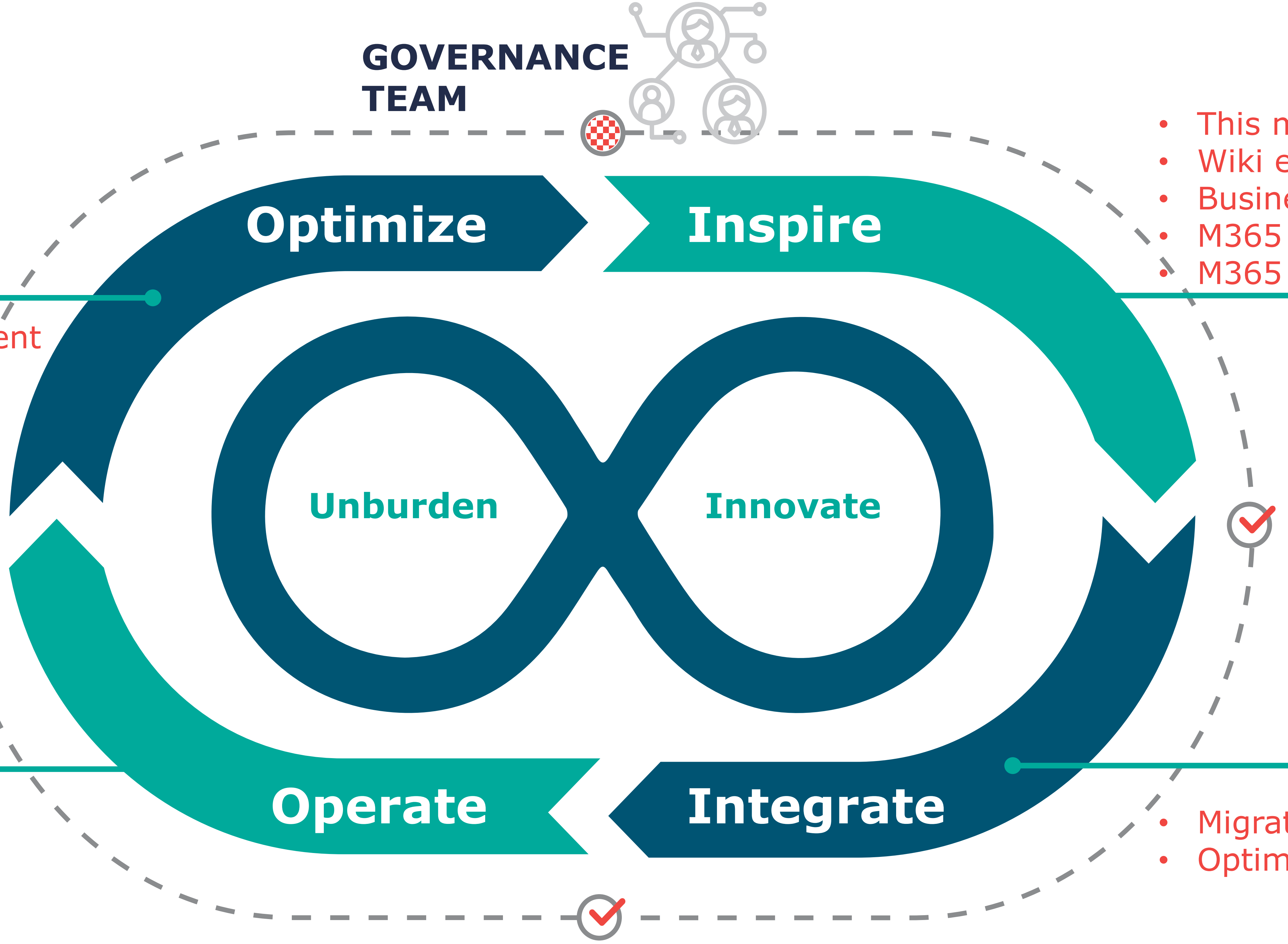
Praktische afspraken

- Vragen via chat
- Iedereen op mute
- Q&A na de presentatie
- Evaluatie met link naar de slides worden na het event doorgestuurd

inetum realdolmen

Positive digital flow

Zero Trust - Identity



GOVERNANCE TEAM

Optimize

Inspire

Unburden

Innovate

Operate

Integrate

- This meeting
- Wiki events
- Business Productivity Roadmap
- M365 Roadmap
- M365 Jumpstart

- Security Priority Assessment
- Calling Assessment
- Proactive Services
- Training, user adoption, change management

- Managed Services
- Workplace as a Service

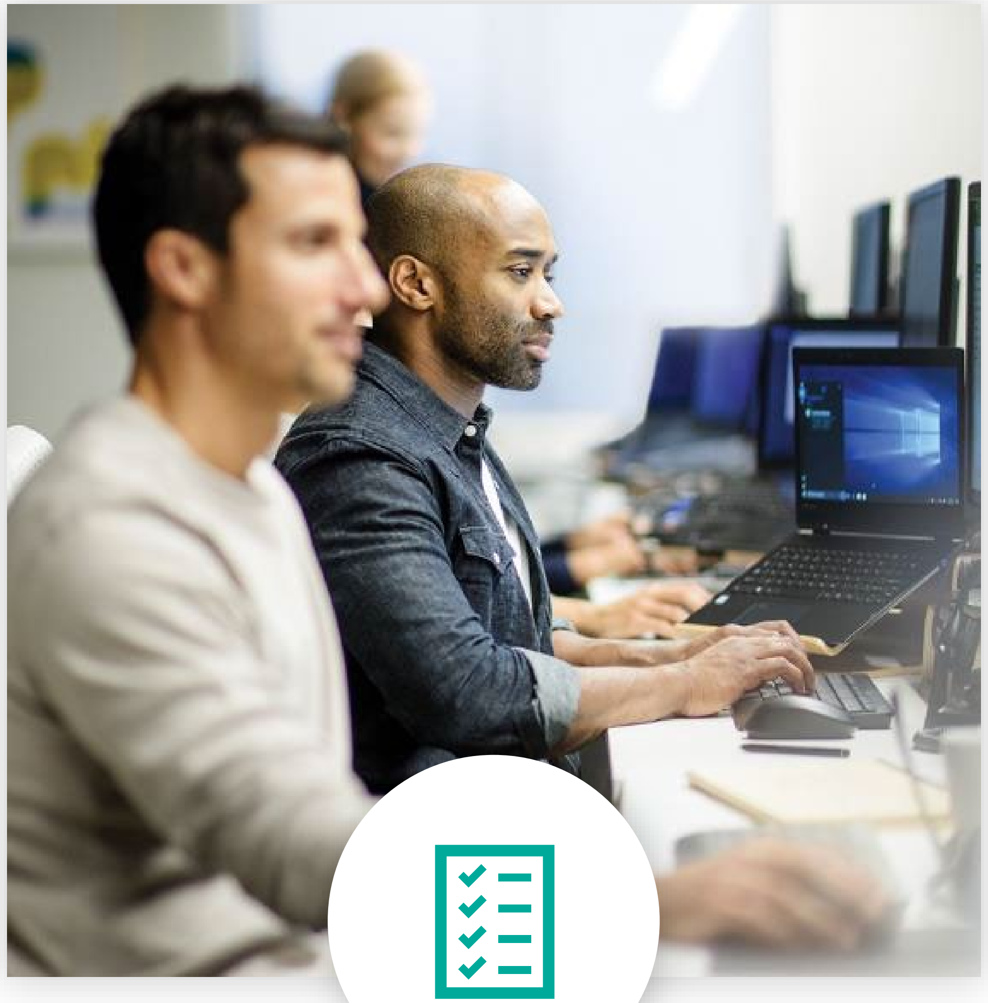
- Migration
- Optimization

Zero Trust Roadmap

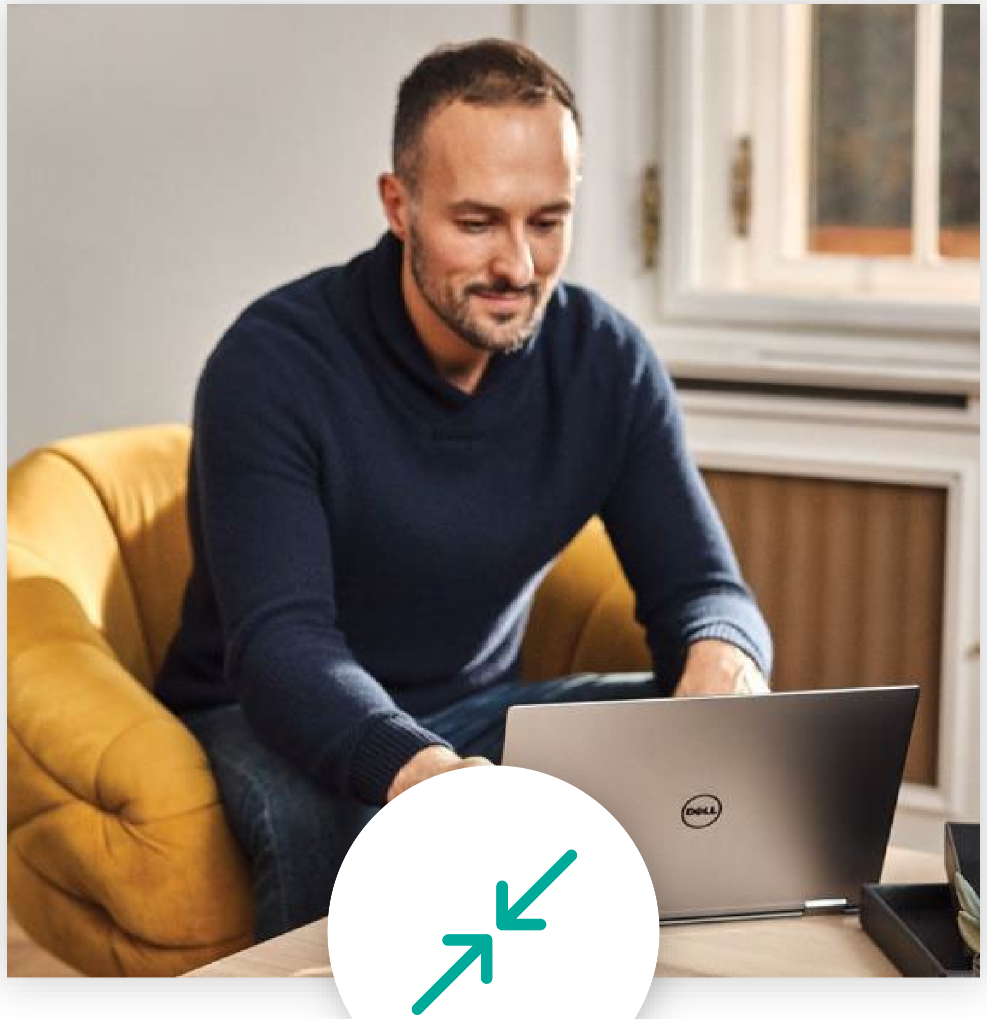
	Identities	Devices	Network & Infrastructure	Applications	Data
TRADITIONAL	No SSO between cloud and on-premises apps Visibility into identity risk is very limited	Devices are domain joined No overview and inventory of devices	Flat open network with unencrypted traffic Minimal threat protection	On-premises apps and no cloud apps No overview of shadow IT	Access is governed by perimeter Unencrypted and without classification
ADVANCED	Basic conditional access policies with basic MFA Cloud identity federation and visibility into identity risk	Devices are registered with a cloud identity provider DLP policies for BYOD	Basic network segmentation Cloud native filtering and threat protection	Apps configured with SSO + discover shadow IT Critical apps are monitored	Access is governed by classification Encrypted and classified via keywords
OPTIMAL	Password less authentication Phishing-proof MFA User behavior is analyzed in real time Enforce least privilege access	Endpoint threat protection is used to monitor device risk Access control is gated on device risk Continuous risk-based asset management	Micro segmentation ML-based threat protection and filtering All traffic is encrypted	Apps are available using least privilege access In-session monitoring and response Assess the security posture of cloud apps	Classification by AI DLP policies based on classification Access governed by cloud security policy engine

← Visibility, analytics, automation & governance →

A new reality needs new principles



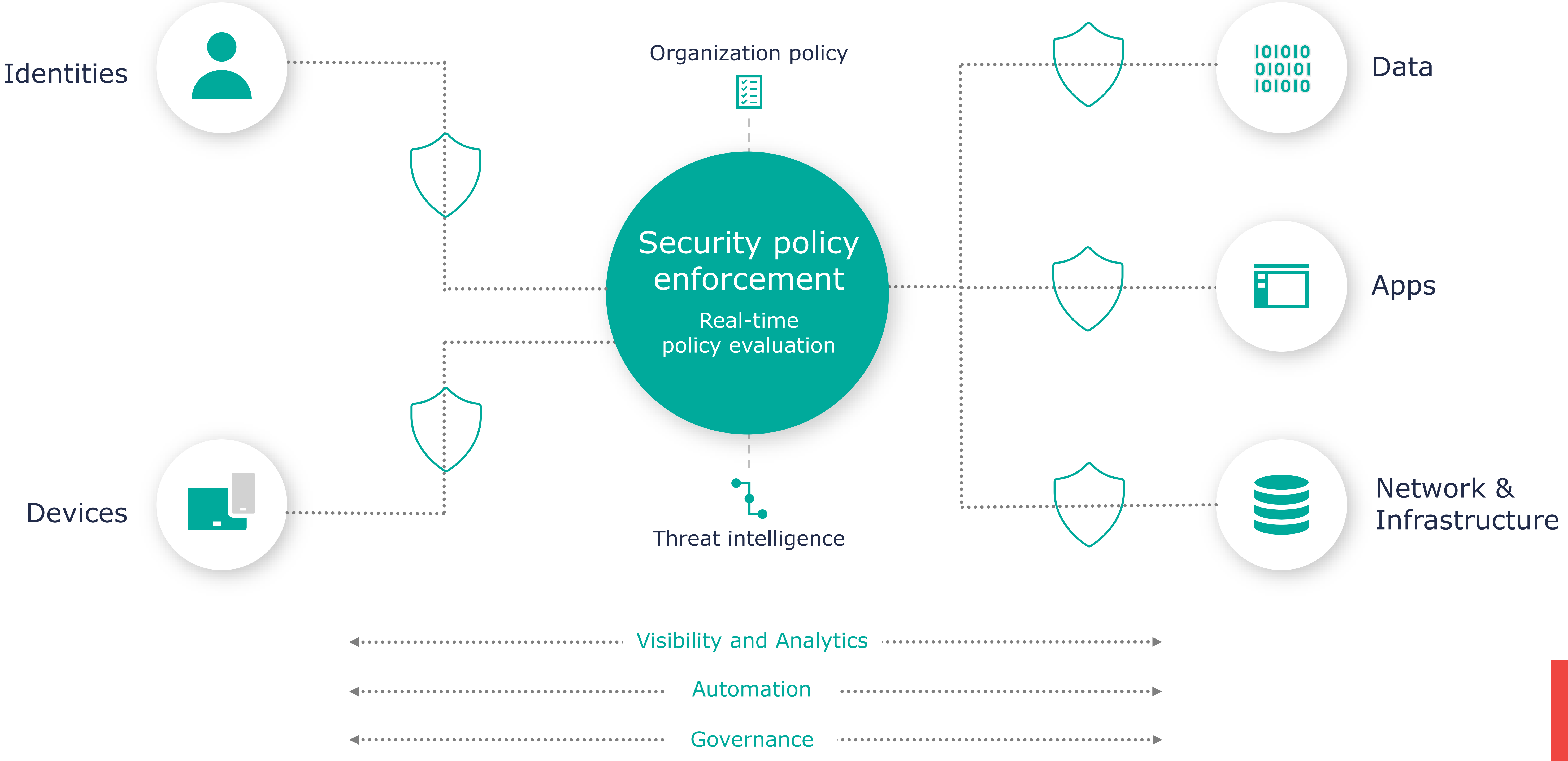
Verify explicitly



Use least privilege access

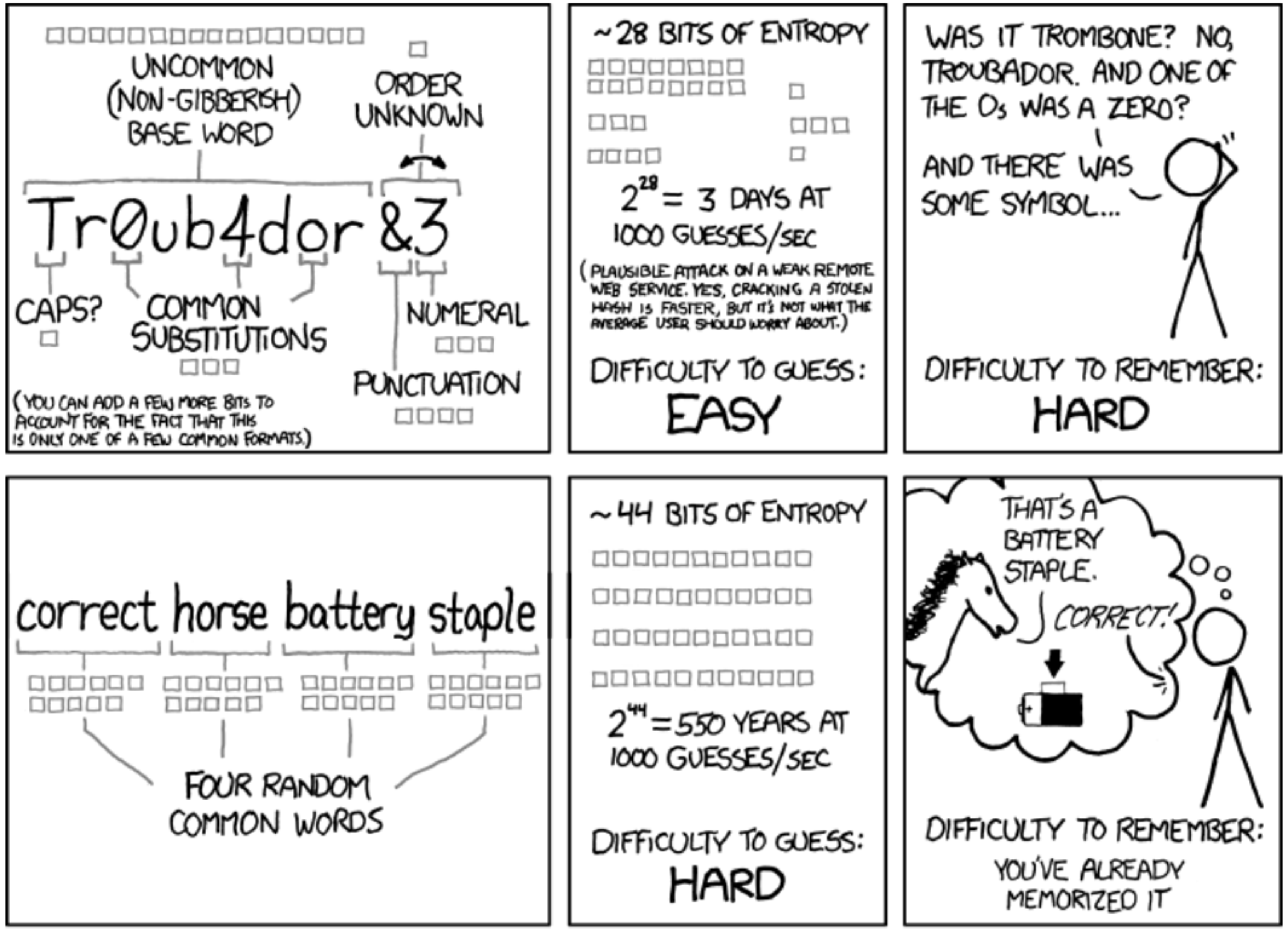
Assume breach

Zero Trust Architecture

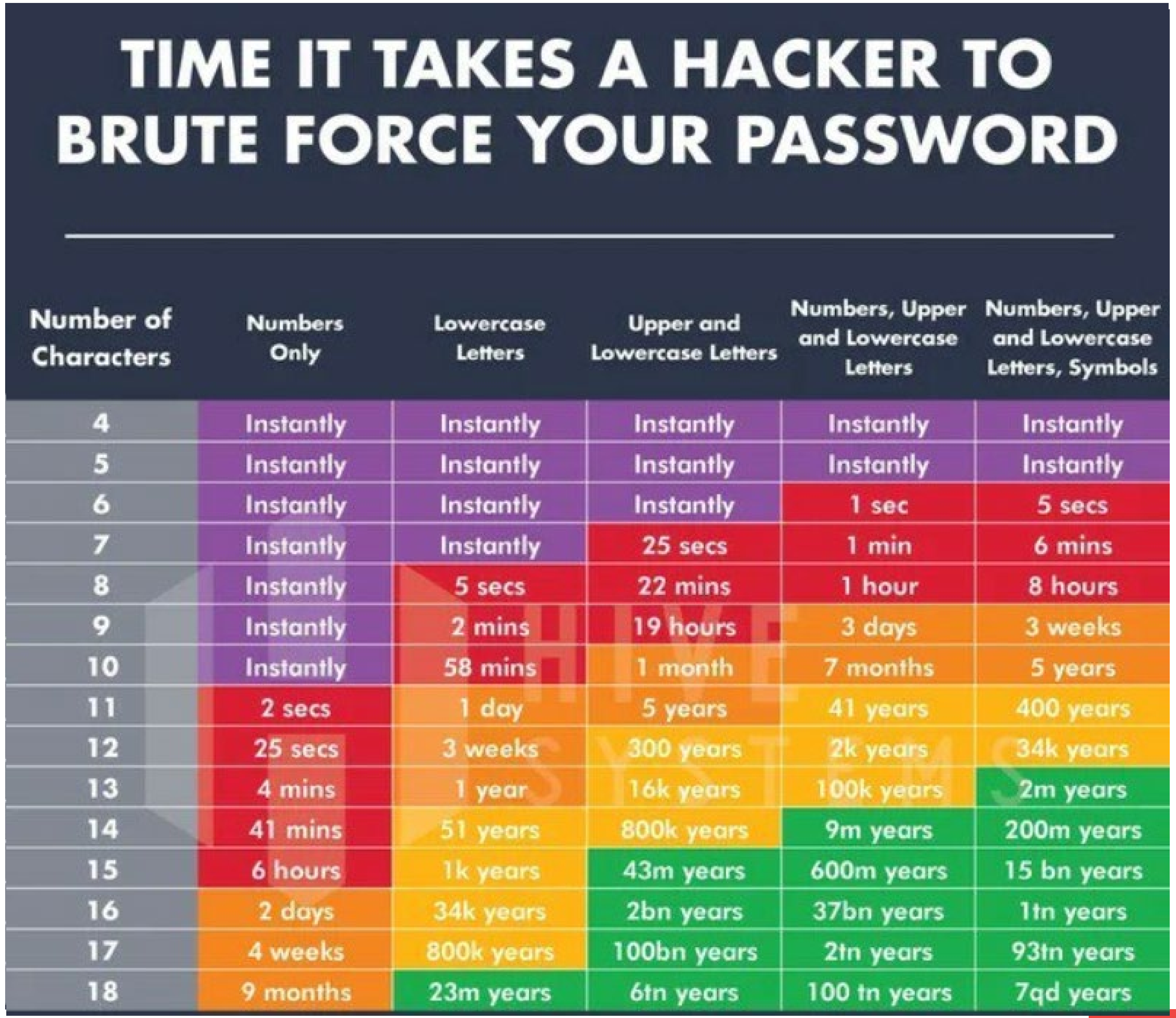


Passwords, the first step to Security?

inetum realdolmen
Positive digital flow


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

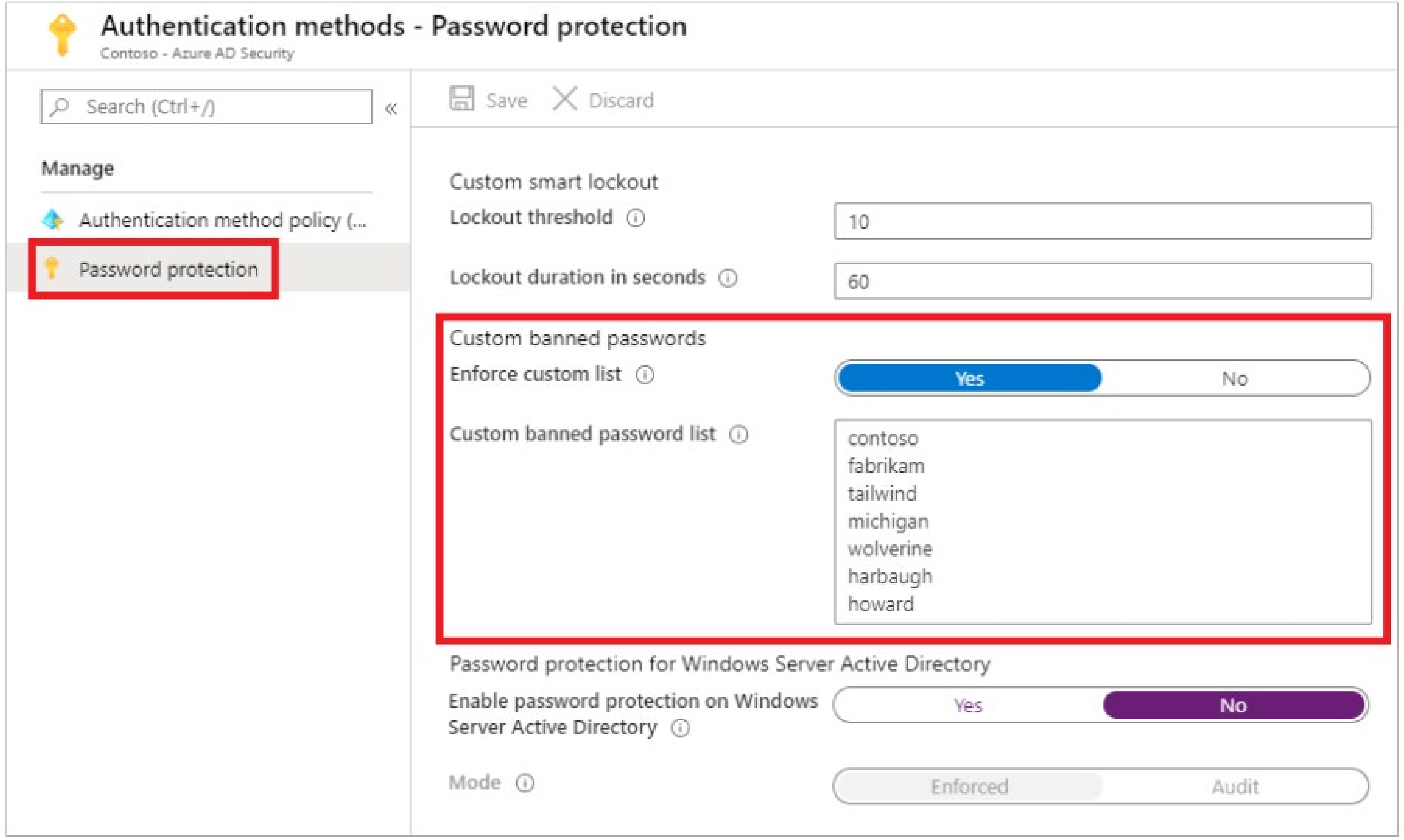
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Ban bad passwords: Password Protection



Authentication methods - Password protection

Contoso - Azure AD Security

Custom smart lockout

Lockout threshold: 10

Lockout duration in seconds: 60

Custom banned passwords

Enforce custom list: [✓ Yes] No

Custom banned password list:

```
contoso
fabrikam
tailwind
michigan
wolverine
harbaugh
howard
```

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory: Yes [✓ No]

Mode: Enforced Audit

- Global Banned Password list
  - Derived from Azure AD security telemetry Data
- Custom Banned Password list
  - Add words that apply to your brands, products, etc…
  - Is smart enough to see replacement of letters with numbers or special characters through normalization

Multifactor Authentication

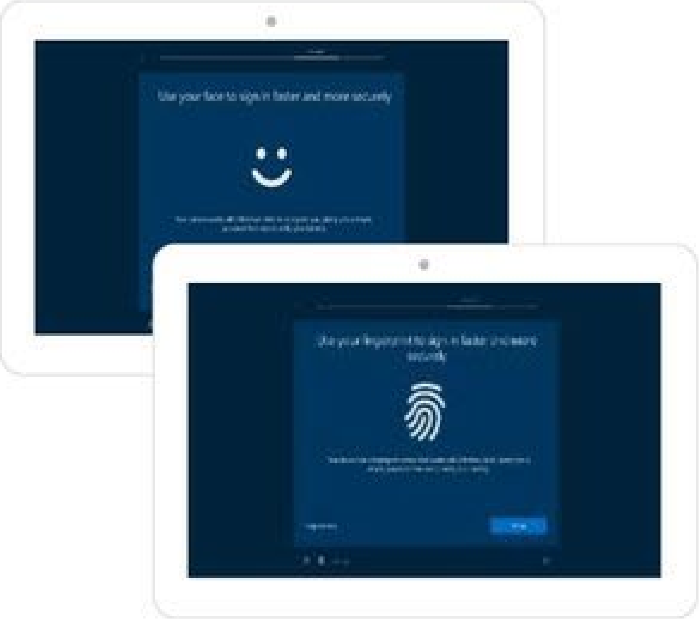
Bad Password (Only)	Good Password +	Better Password +	Best | Passwordless
123456	SMS	Authenticator (Push notifications)	Windows Hello
qwerty	Voice	Software Tokens OTP	Authenticator (Phone Sign-in)
password		Hardware Tokens OTP (Preview)	FIDO2 security key
Iloveyou			
Password1			

Windows Hello Experience

Enrollment

Setup Process

In OOBE but can also be launched via settings.



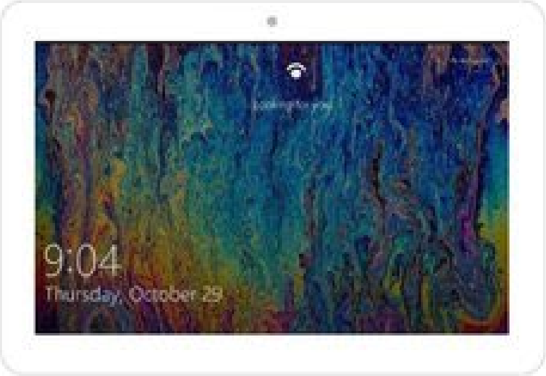
Use your face to sign in faster and more securely

Use your fingerprint to sign in faster and more securely

Login

Device Unlock

Upon boot or resume, use your biometric to unlock your device



Looking for you

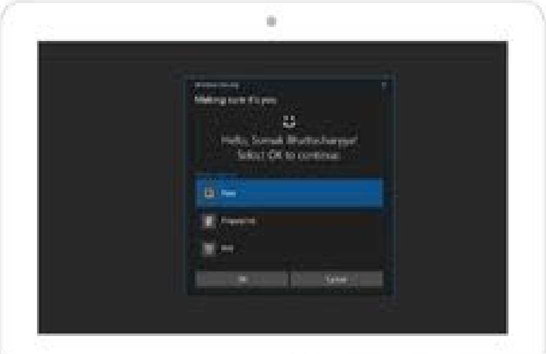
9:04

Thursday, October 29

Re-auth

App or Website

As credentials are needed, apps or websites can request to verify you are using your device.



Making sure it's you

Hello, Somak Bhattacharyya!
Select OK to continue.

Hello Miranda Vance

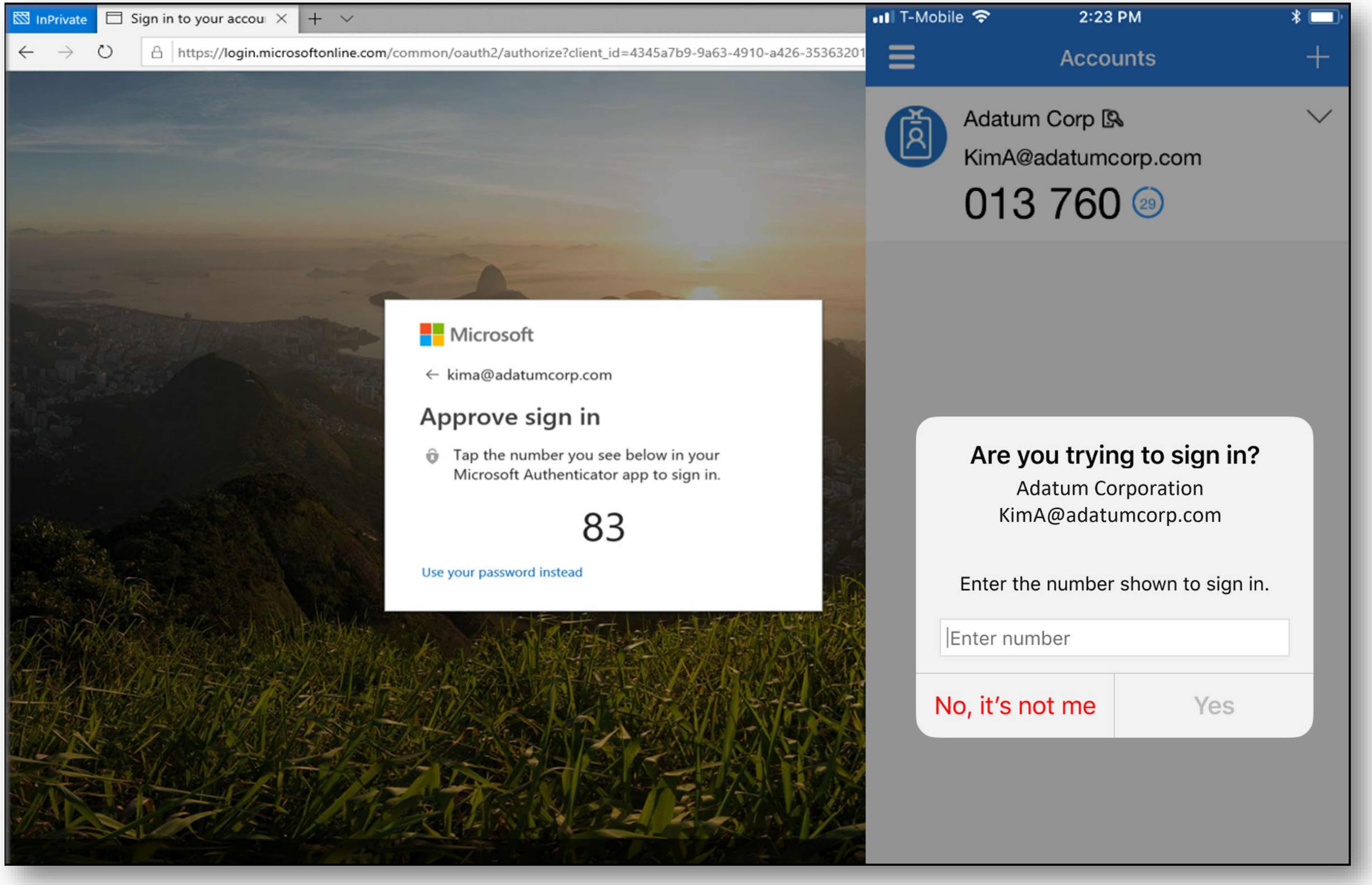
6:30

Thursday, July 30

Lunch with Barbra
Café
11:00 AM—12:00 PM

Authenticator Advanced Features (Generally Available)

Number matching & Additional Context – prevent accidental approvals



InPrivate | Sign in to your accou

https://login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201

Microsoft

← kima@adatumcorp.com

Approve sign in

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

83

Use your password instead

T-Mobile 2:23 PM

Accounts

Adatum Corp

KimA@adatumcorp.com

013 760 29

Are you trying to sign in?

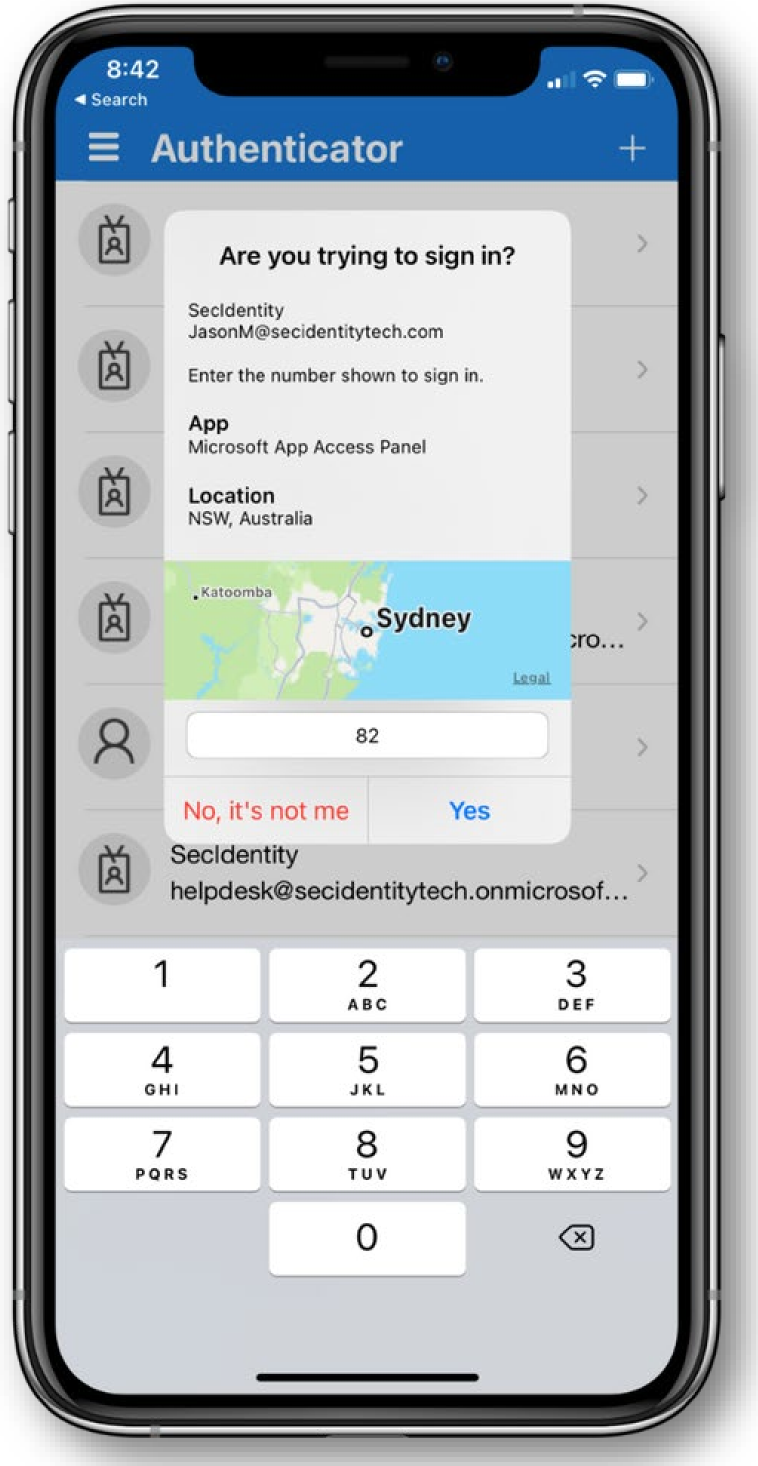
Adatum Corporation

KimA@adatumcorp.com

Enter the number shown to sign in.

Enter number

No, it's not me | Yes



8:42

◂ Search

Authenticator

Are you trying to sign in?

SecIdentity

JasonM@secidentitytech.com

Enter the number shown to sign in.

App
Microsoft App Access Panel

Location
NSW, Australia

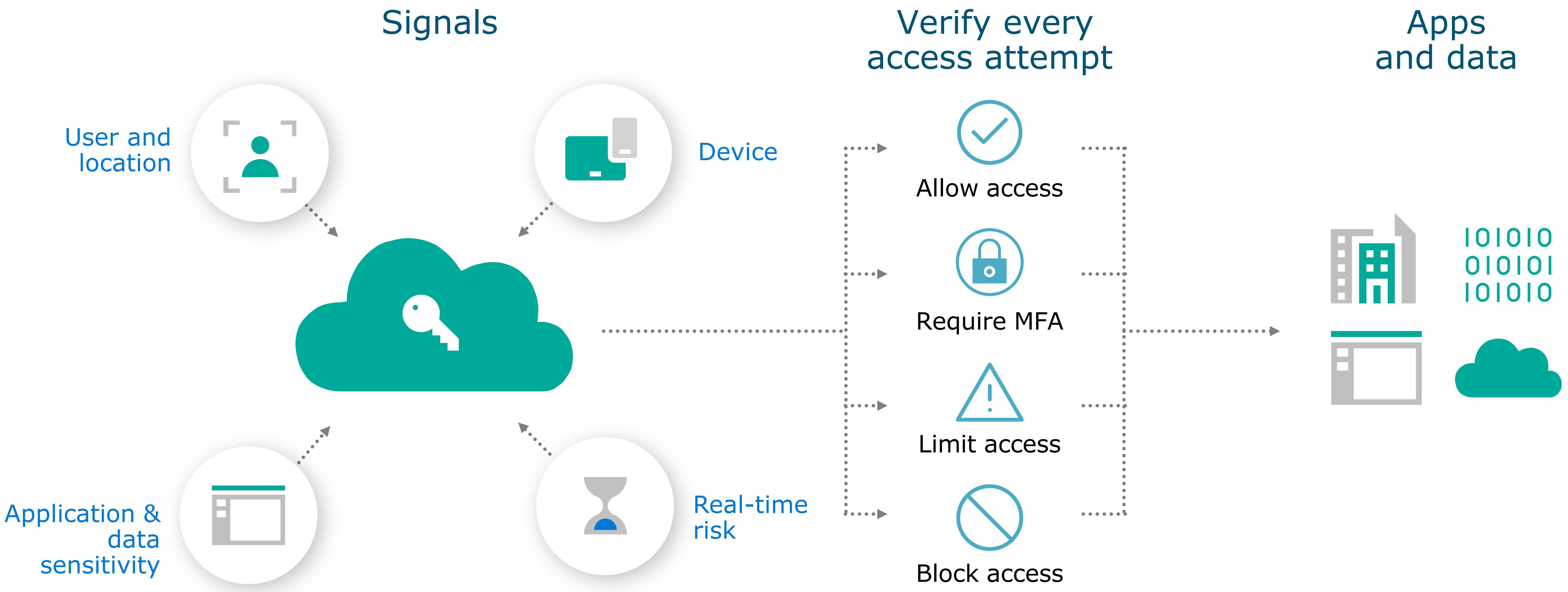
82

No, it's not me | Yes

SecIdentity

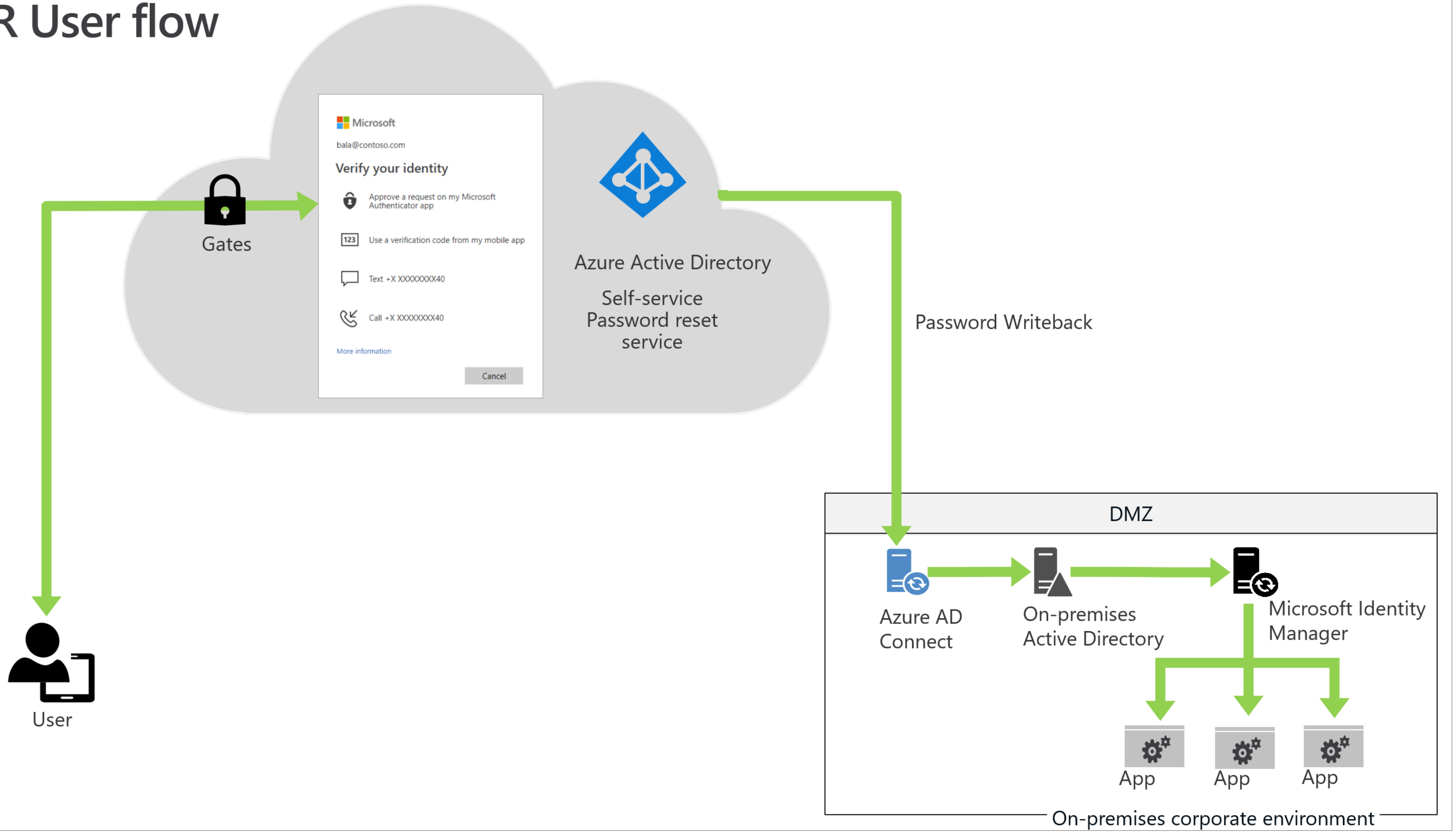
helpdesk@secidentitytech.onmicrosof…

Control access with smart policies and risk assessments



Self Service Password Reset

SSPR User flow



Microsoft

bala@contoso.com

Verify your identity

Approve a request on my Microsoft Authenticator app

Use a verification code from my mobile app

Text +X XXXXXXXX40

Call +X XXXXXXXX40

More information

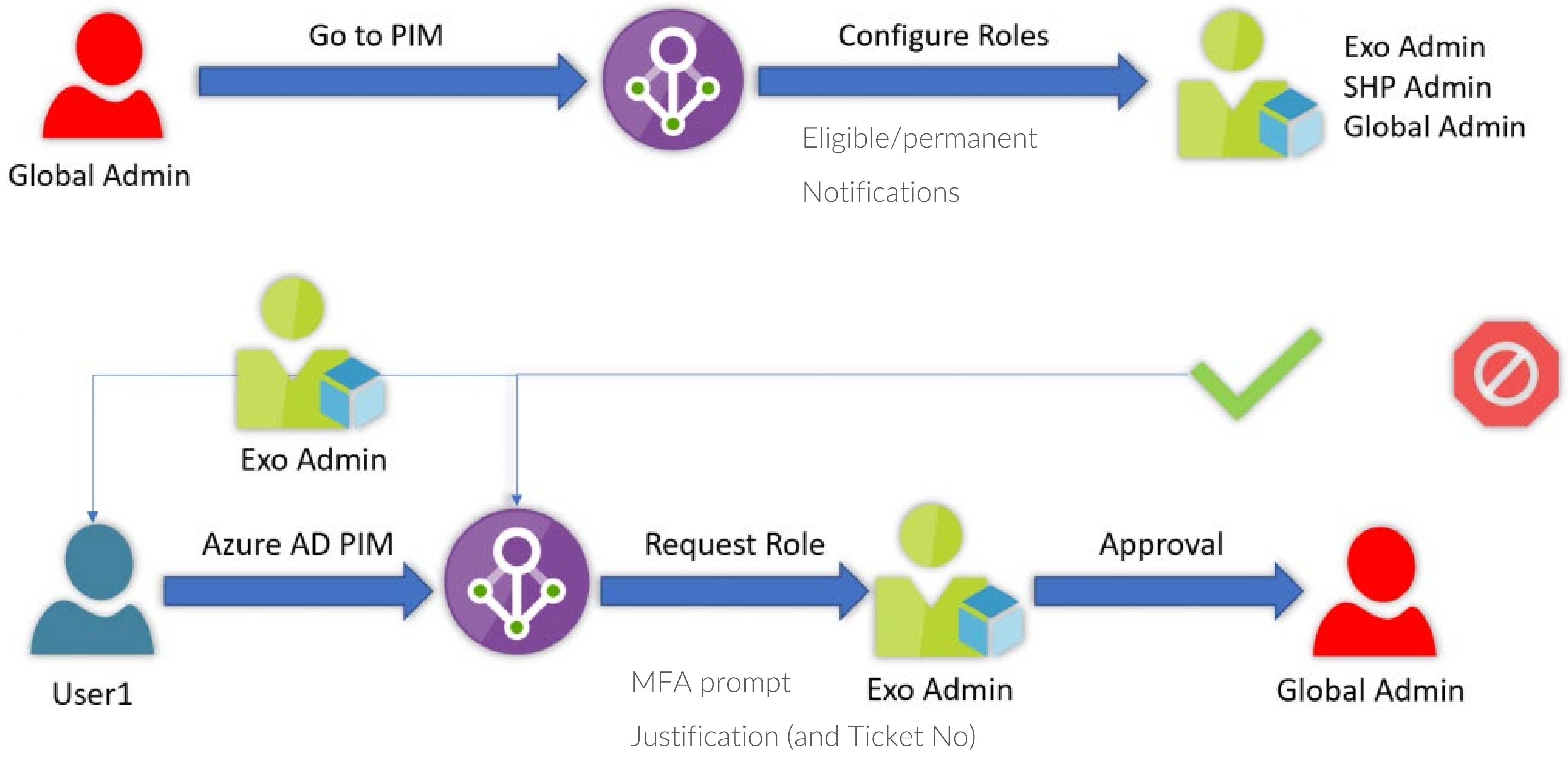
Cancel

Gates
Azure Active Directory
Self-service Password reset service
Password Writeback
User
DMZ
Azure AD Connect
On-premises Active Directory
Microsoft Identity Manager
App
App
App
On-premises corporate environment

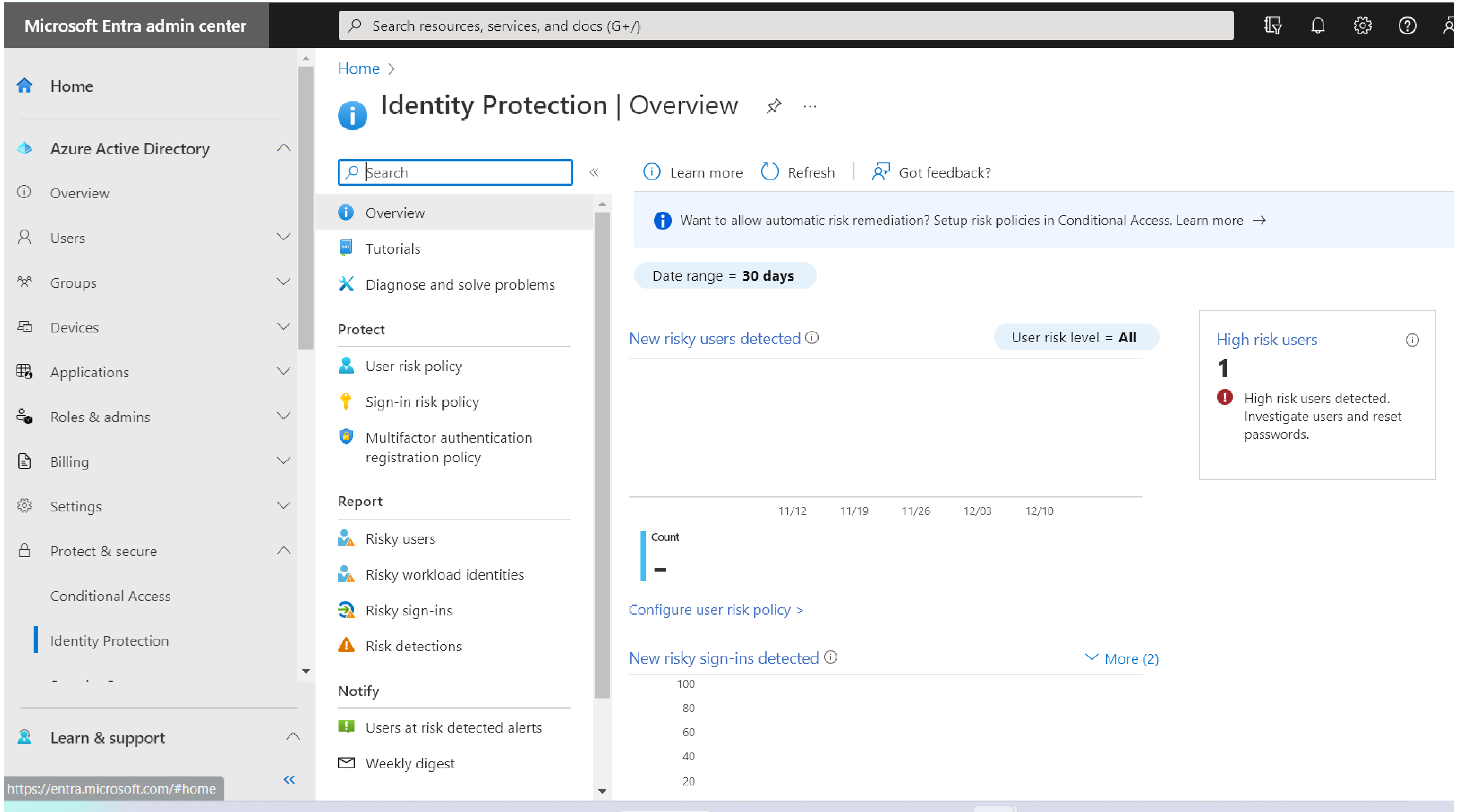
Privileged Identity Management

Manage, control and monitor access to important resources

- ✓ Time-bound Privileged Access (JIT)
- ✓ Approval Flow possibilities
- ✓ Leverage MFA to validate requestor
- ✓ Auditing / Discovery & Insights
- ✓ Leverage Access Reviews
- ✓ M365 roles and Azure resources
- ✓ Privilege Access Groups (Preview)
- ✓ Azure AD Premium 2 License (MAU!)



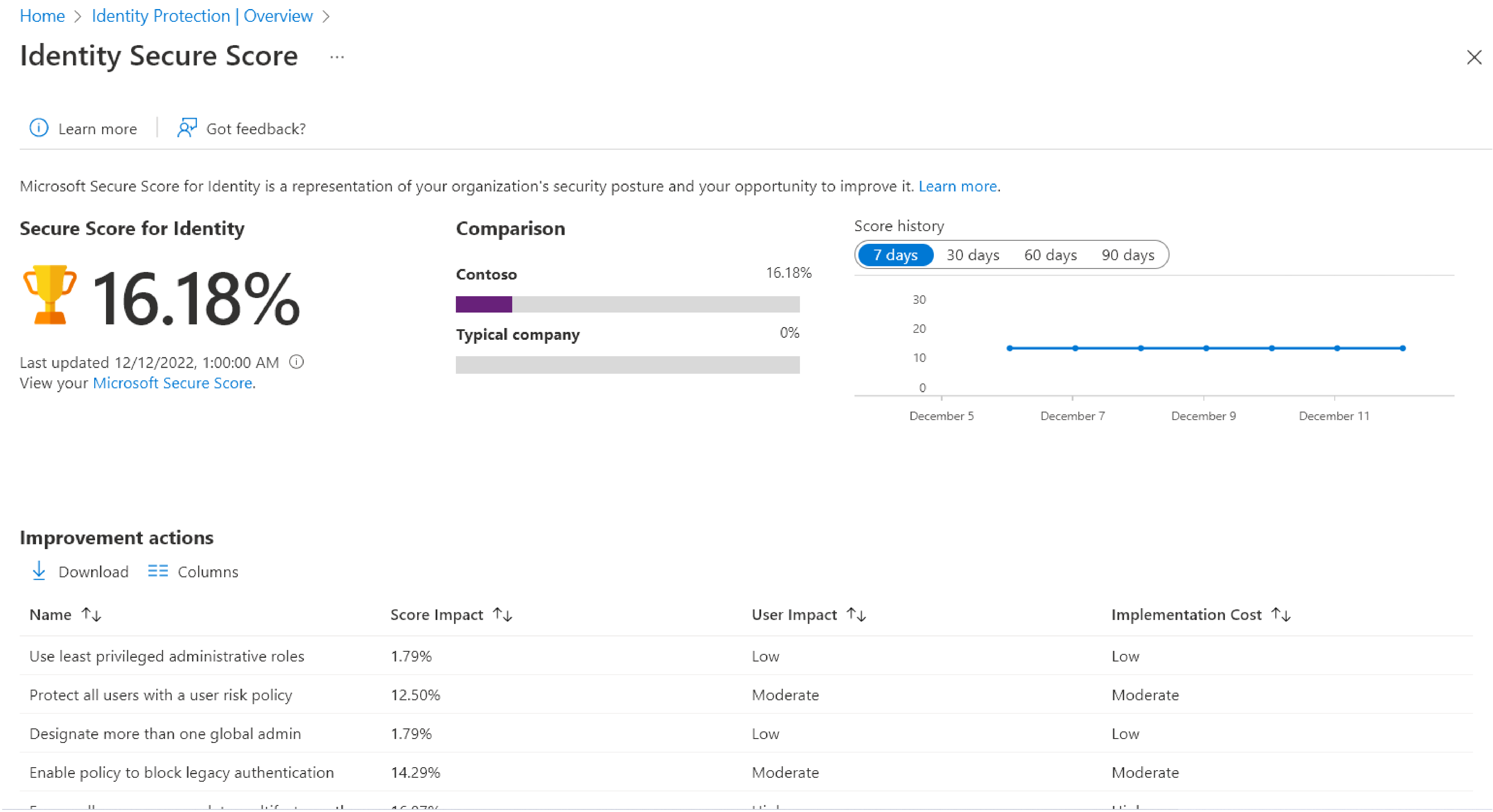
Entra.microsoft.com



Want to allow automatic risk remediation? Setup risk policies in Conditional Access. Learn more →

High risk users detected. Investigate users and reset passwords.

Identity Secure Score



Identity Secure Score

Microsoft Secure Score for Identity is a representation of your organization's security posture and your opportunity to improve it. Learn more.

Secure Score for Identity

16.18%

Last updated 12/12/2022, 1:00:00 AM
View your Microsoft Secure Score.

Comparison

Contoso	16.18%
Typical company	0%

Score history

Improvement actions

Name ↑↓	Score Impact ↑↓	User Impact ↑↓	Implementation Cost ↑↓
Use least privileged administrative roles	1.79%	Low	Low
Protect all users with a user risk policy	12.50%	Moderate	Moderate
Designate more than one global admin	1.79%	Low	Low
Enable policy to block legacy authentication	14.29%	Moderate	Moderate

Zero Trust Roadmap Identities

TRADITIONAL

- Several identity providers are in use,
- No SSO is present between cloud and on-premises apps
- Visibility into identity risk is very limited

ADVANCED

- Cloud identity federates with on-premises systems
- Basic conditional access policies implemented
- Visibility into identity risk with analytics
- Enforce basic MFA

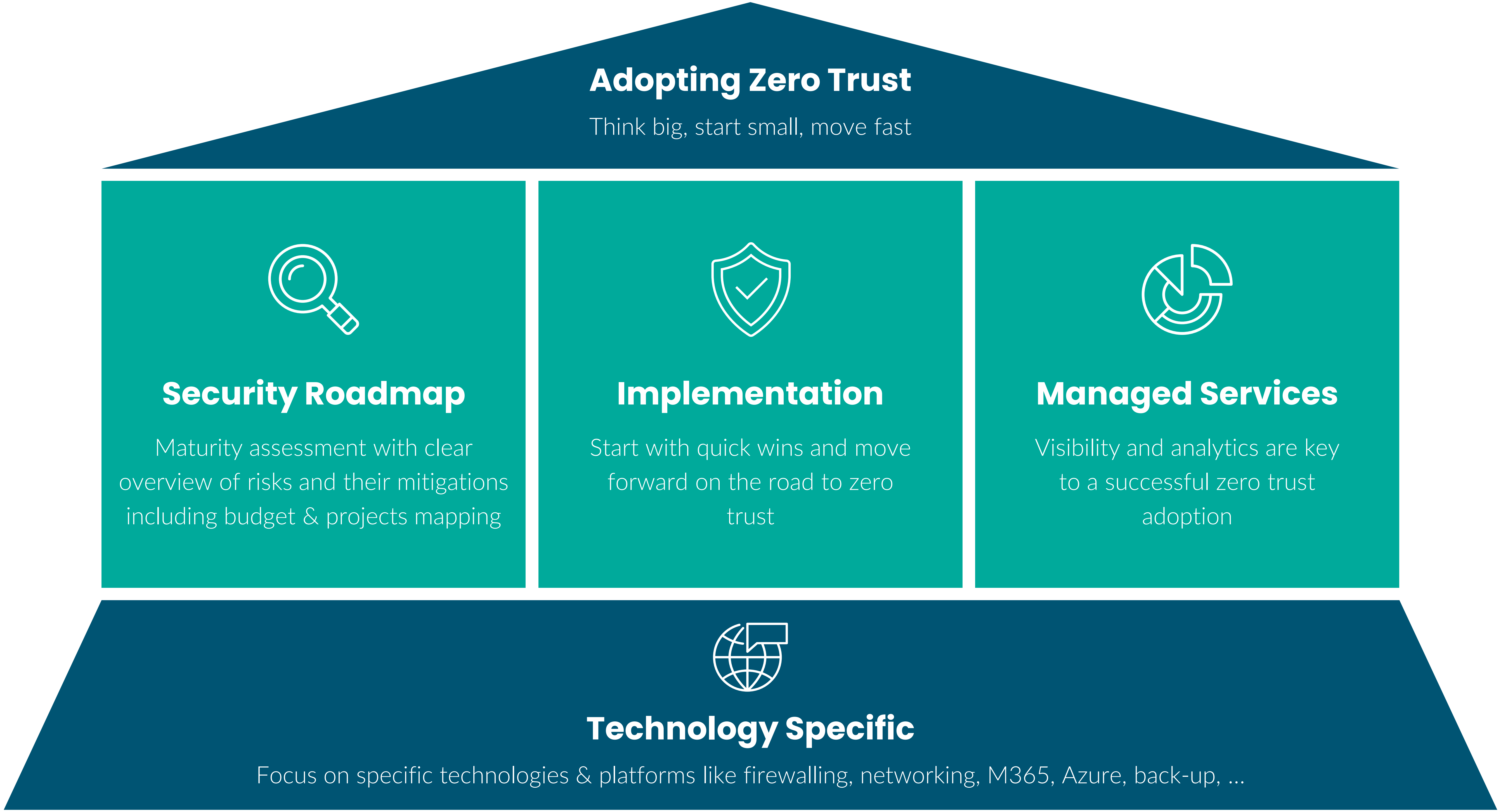
OPTIMAL

- Passwordless authentication is enabled
- Phishing-proof MFA is enforced
- User behavior is analyzed in real time to determine risk
- Enforce least privilege access with strong governance

inetum
realdolmen
Positive digital flow

Q&A

Security adoption



Adopting Zero Trust

Think big, start small, move fast

Security Roadmap

Maturity assessment with clear overview of risks and their mitigations including budget & projects mapping

Implementation

Start with quick wins and move forward on the road to zero trust

Managed Services

Visibility and analytics are key to a successful zero trust adoption

Technology Specific

Focus on specific technologies & platforms like firewalling, networking, M365, Azure, back-up, …

Toekomstige webinars rond Zero Trust

25/01	Privileged accounts: een gemakkelijk doelwit voor hackers?
01/02	Hou grip op uw documenten met Azure Information Protection
08/02	Microsoft 365 Defender Threat Protection: een gedegen security-oplossing
15/02	Aan de slag met big data? Beheer de overvloed aan data met Azure Purview

www.inetum-realdolmen.world/nl/events

Contacteer ons via:

- info@inetum-realdolmen.world
- Uw vertrouwde contactpersoon bij Inetum-Realdolmen
- Evaluatieformulier