



# **Saving Your Butt:** **The many layers of Identity Protection**

Alexander Solaat Rødland & Olav Tvedt



PLATINUM

resco

 AvePoint®

**PROMISE**  
GRUPA APN PROMISE

502nm

**NRGW**

  
EUROPEAN CLOUD SUMMIT

SILVER

GOLD

 pax8

**Visit Tallinn**

 Sparkle



NORDIC KOOLITUS

**ESPC**

FORCEWORKS  GLOBAL

BRONZE



QUBIX

 Digital

 CRMK

**DY  
NAM  
ICS** MINDS

 netspore

  
ColorCloud  
HAMBURG

WORKSHOPS

COMMUNITY

# Remember to take pictures, post on X / LinkedIn!

## #CTTT24

---

### Agenda



- Who are you – 101 identification and access
- What is MEID and where is that typo?
- Authentication methods
  - And their chicken-and-egg-problems
- Why p@\$w0rds s\*\*\* and what you can't do about it
- What you need to learn from Popeye



# Alexander Solaat Rødland (him/he)

Principal Cloud Engineer @ Fortytwo, NO

It's easier to stay out, than get out!



[alexander@solaat.no](mailto:alexander@solaat.no)



[youtube.com/@bluescreenbrothers](https://youtube.com/@bluescreenbrothers)



[@alexolaat](https://twitter.com/alexolaat)



[/in/alexolaat](https://in.linkedin.com/in/alexolaat)



## Olav Tvedt (him/he)

Cloud dude @ Sparebanken Vest, NO

Simplicity is a difficult thing to achieve!  
- Charlie Chaplin



[olav@tvedt.info](mailto:olav@tvedt.info)



[youtube.com/@bluescreenbrothers](https://youtube.com/@bluescreenbrothers)



[@OlavTwitt](https://twitter.com/OlavTwitt)



[/in/otvedt](https://in.linkedin.com/in/otvedt)

# Who are you?



# What are you accessing?



Getting 'modern'





# Where is Waldo?

- Any calls from «Microsoft» lately?



# Evolution of identity and access?



# Evolution of identity and access?

...As the prophecy of Dall-E...

Egyptians

Romans

Monarchy

Active Directory

Azure Active Directory

Entra ID



# ABSI (Artificial Butt-Saving Intelligence)

- Block identity takeover in real-time



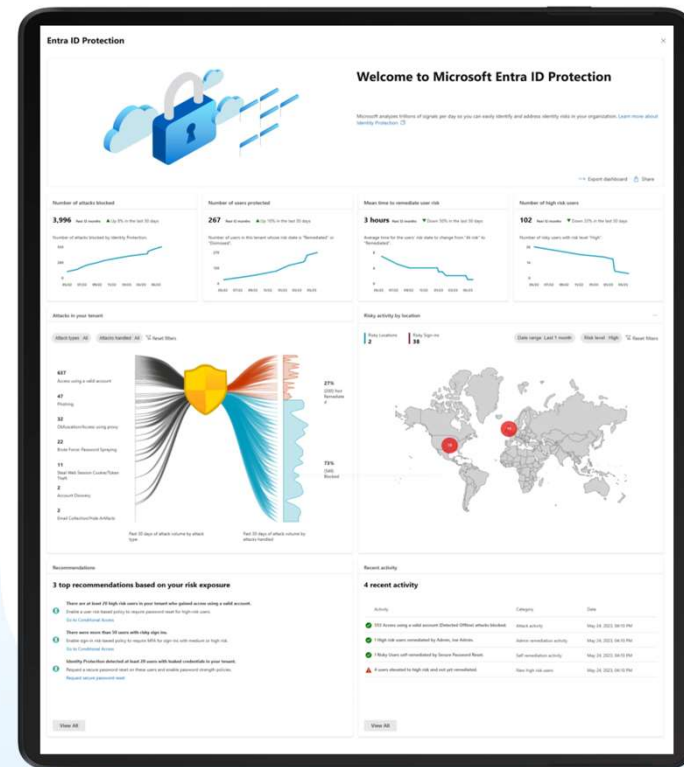
Prevent identity compromise



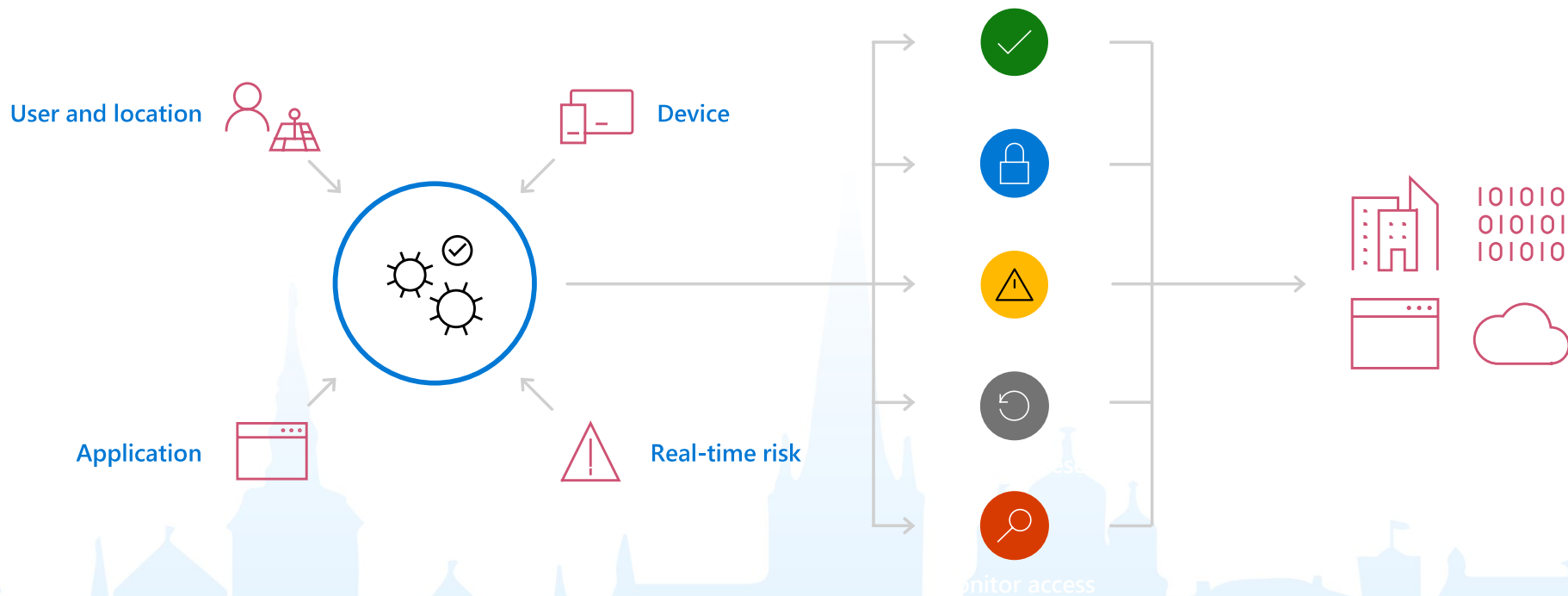
Enforce policies

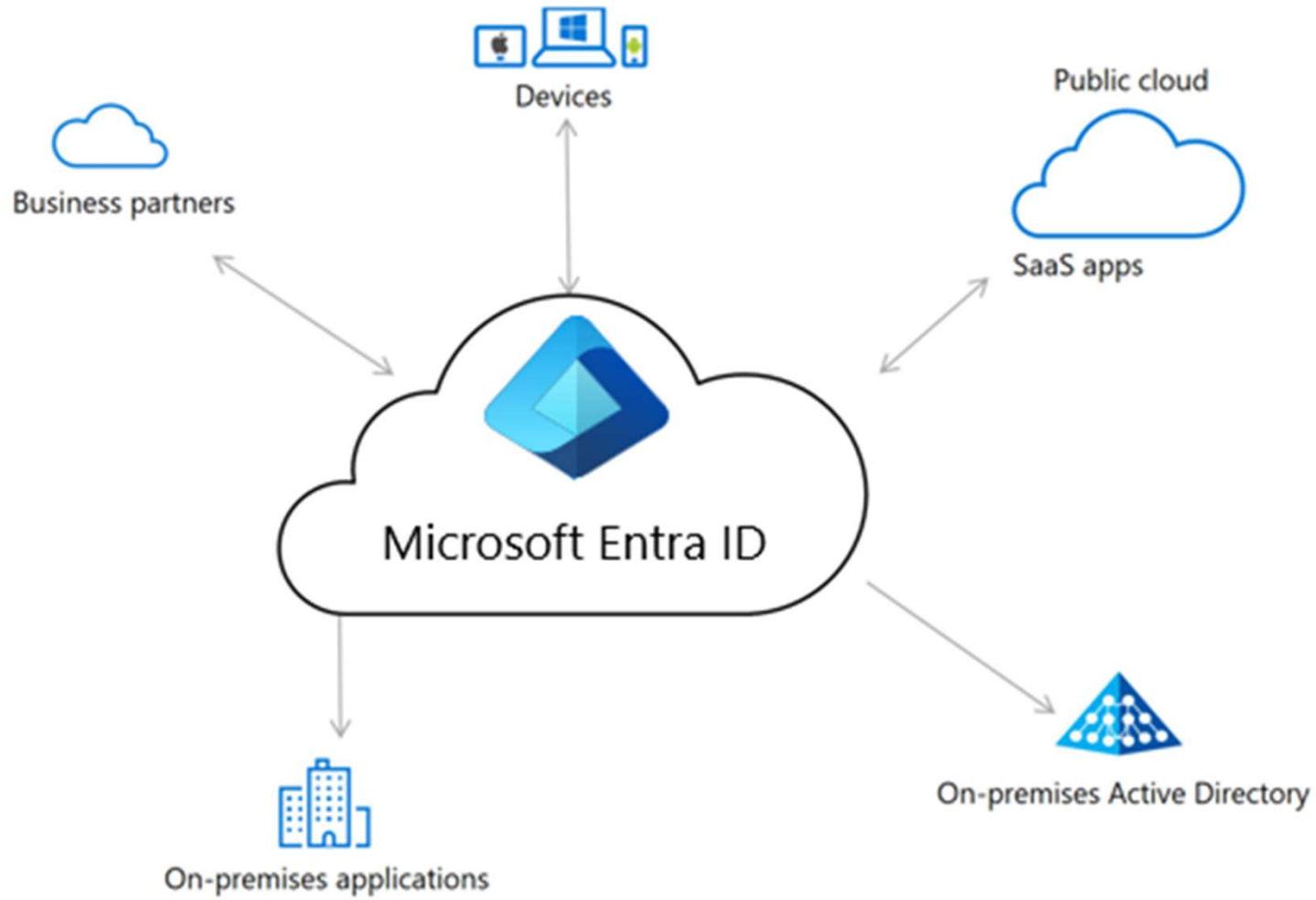


Seamlessly integrate



# 40TB of butt-saving security signals







# Microsoft Entra ID

## "Plans"

Microsoft Entra ID Free

Microsoft Entra ID P1

Included in Microsoft 365 E3

Microsoft Entra ID P2

Identity P2 = Identity P1 + Identity Protection

Included in Microsoft 365 E5

## Why identity

- Authentication
  - Who they are
- Authorization
  - What they can do
- Auditing
  - What they did
- Administration
  - Maintenance



# Microsoft Entra ID

## "Plans"

Microsoft Entra ID Free

Microsoft Entra ID P1

Included in Microsoft 365 E3

Microsoft Entra ID P2

Identity P2 = Identity P1 + Identity Protection

Included in Microsoft 365 E5

## "Add-Ons"

Microsoft Entra ID Governance

Microsoft Entra Verified ID

Microsoft Entra Permissions  
Management

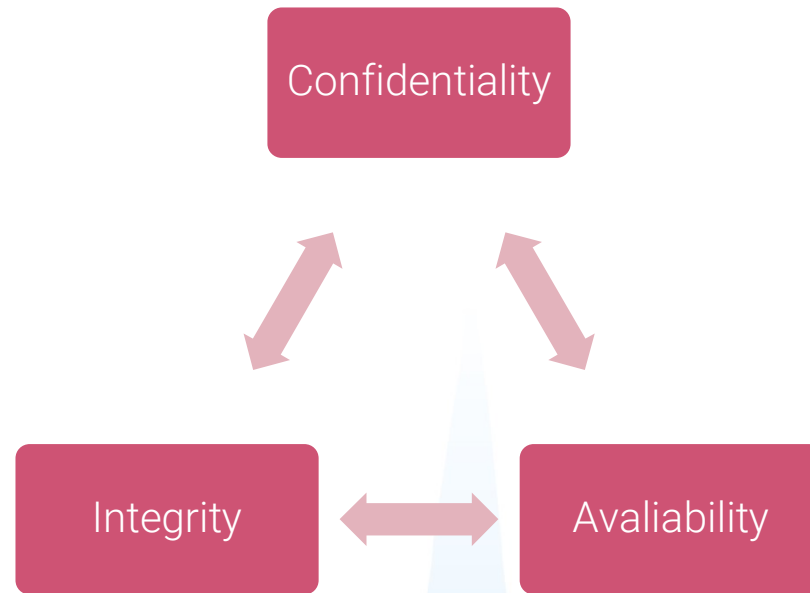
Microsoft Entra Workload ID



# Identity security considerations




# CIA



# Administrative units

- Can only contain users, groups, and devices.
- Restricts permissions to a defined portion of your organization

## Add administrative unit ...












 Got feedback?

Properties Assign roles Review + create

### Administrative roles

Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. [Learn more](#)

Role ↑↓

-  Authentication Administrator
-  Cloud Device Administrator
-  Groups Administrator
-  Helpdesk Administrator
-  License Administrator
-  Password Administrator
-  Printer Administrator
-  SharePoint Administrator
-  Teams Administrator
-  Teams Devices Administrator
-  User Administrator



User Admini



# A random person from the audience

A brave person...

# What are access packages? What can I manage with them?

- List of resources such as groups, apps, and sites,
- Adds the roles a user needs for those resources.
- Policy controlled rules for who can access the package.

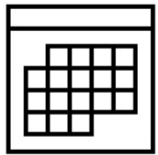


Thank you Marius!  
A brave random person



# When should I use access packages?

Time-limited  
access



Manager approval  
or delegated  
role / identity



Manage access  
without IT  
involvement



Cross-organization  
collaboration





# What's in it for me?

## Active Directory

- Basic catalog service
- Authentication
- Access control
- Limited security

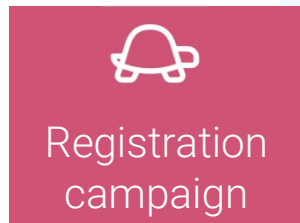
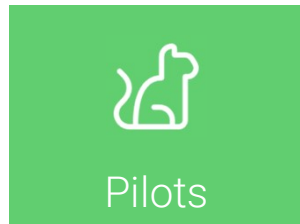
## Azure Active Directory

- Evolved catalog service
- MFA Authentication
- Tokens
- Service principals
- Stronger security

## Microsoft Entra ID

- Modern catalog service
- Strong MFA
- Tokens
- Service principals
- Stronger security
- ME \* Access

# Supported methods



Microsoft Entra admin center

Search resources, services, and docs (G+)

alexander@solaat.one  
CONTOSO (SOLAAT.ONE)

Home > Authentication methods | Policies >

## FIDO2 security key settings

FIDO2 security keys are a phishing-resistant, standards-based passwordless authentication method available from a variety of vendors. [Learn more.](#)  
FIDO2 keys are not usable in the Self-Service Password Reset flow.

Enable and Target **Configure**

GENERAL

Allow self-service set up  Yes  No

Enforce attestation  Yes  No

KEY RESTRICTION POLICY

Enforce key restrictions  Yes  No

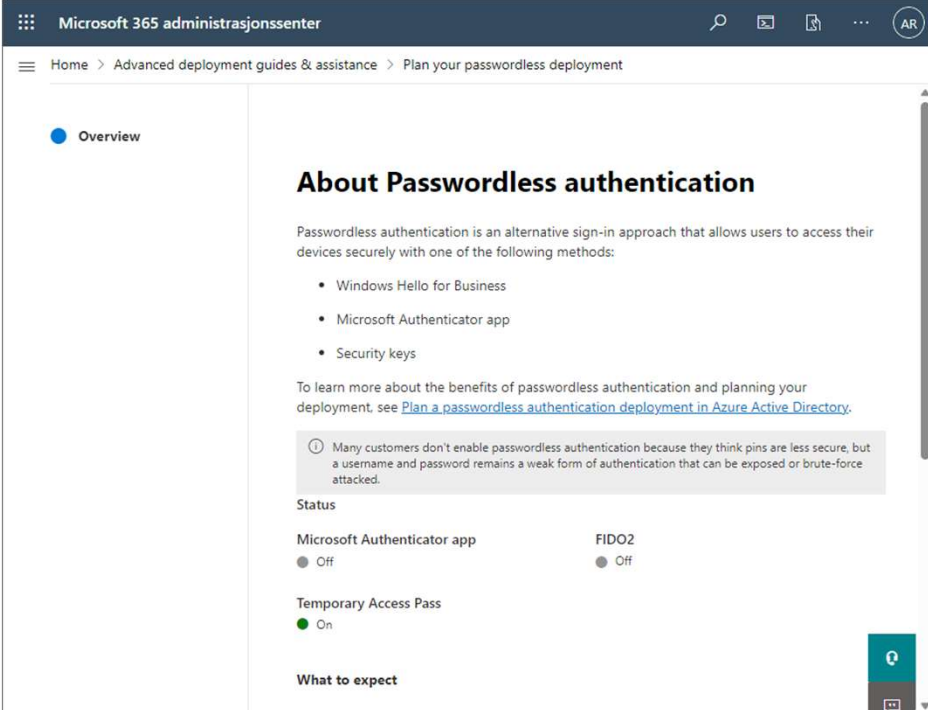
Restrict specific keys  Allow  Block

[Add AAGUID](#)

No AAGUIDs have been added.

# Go passwordless

- <https://aka.ms/passwordlesswizard>



Microsoft 365 administrasjonscenter

Home > Advanced deployment guides & assistance > Plan your passwordless deployment

Overview

## About Passwordless authentication

Passwordless authentication is an alternative sign-in approach that allows users to access their devices securely with one of the following methods:

- Windows Hello for Business
- Microsoft Authenticator app
- Security keys

To learn more about the benefits of passwordless authentication and planning your deployment, see [Plan a passwordless authentication deployment in Azure Active Directory](#).

Many customers don't enable passwordless authentication because they think pins are less secure, but a username and password remains a weak form of authentication that can be exposed or brute-force attacked.

Status

Microsoft Authenticator app  Off

FIDO2  Off

Temporary Access Pass  On

What to expect

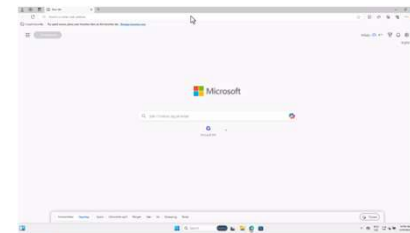
Next Cancel

# Demo: Passwordless

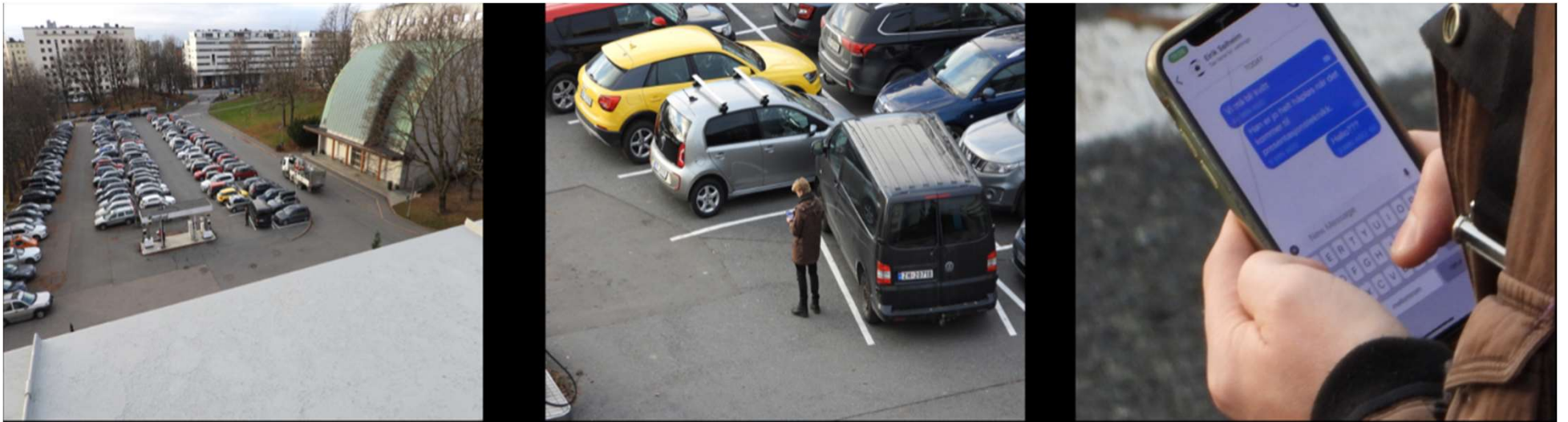
**Fortytwo**  
BY AMESTO



## DEMO TIME



# P@\$\$w0rd?



# Hello vs Hello for Business

## The difference between Windows Hello and Windows Hello for Business

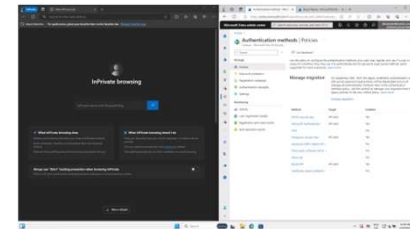
- Individuals can create a PIN or biometric gesture on their personal devices for convenient sign-in. This use of Windows Hello is unique to the device on which it's set up, but can use a password hash depending on an individual's account type. This configuration is referred to as *Windows Hello convenience PIN* and it's not backed by asymmetric (public/private key) or certificate-based authentication.
  - *Windows Hello for Business*, which is configured by group policy or mobile device management (MDM) policy, always uses key-based or certificate-based authentication. This behavior makes it more secure than *Windows Hello convenience PIN*.
- In a nutshell: Windows Hello for Business =  
Windows Hello + the Asymmetric Authentication method

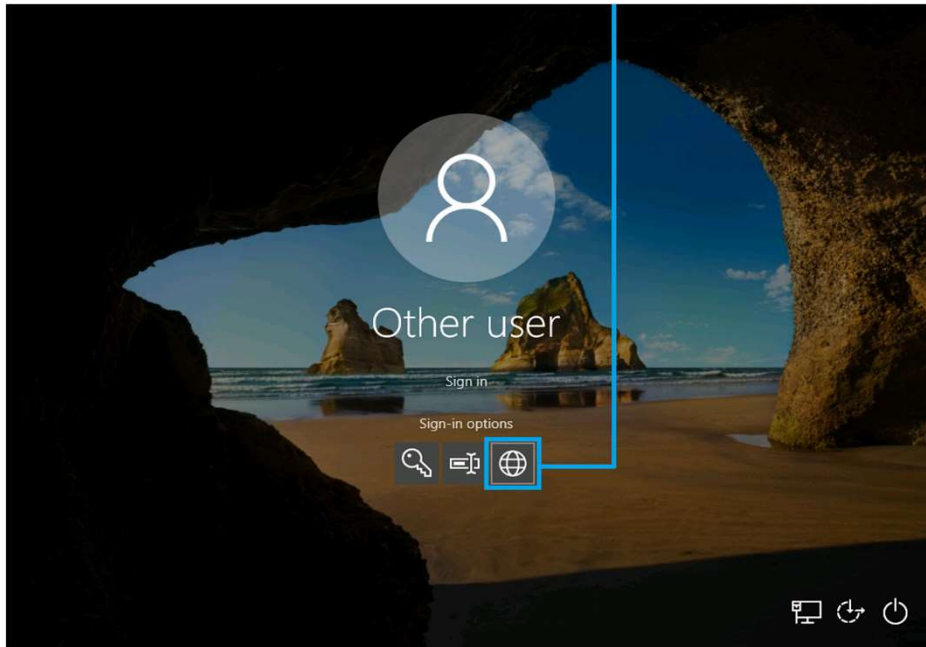
# Demo: TAP

Fortytwo  
BY AMESTO



## DEMO TIME





## For joined devices to Azure AD

- During the domain-join setup process, users can authenticate with a TAP to join the device and register Windows Hello for Business.
- On already-joined devices, users must first authenticate with another method such as a password, smartcard or FIDO2 key, before using TAP to set up Windows Hello for Business.
- If the Web sign-in feature on Windows is also enabled, the user can use TAP to sign into the device. This is intended only for completing initial device setup, or recovery when the user doesn't know or have a password.



Zero  
Trust

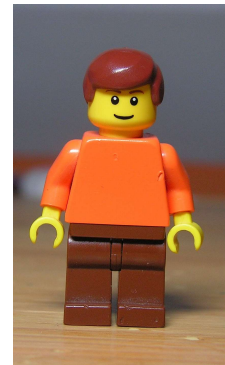
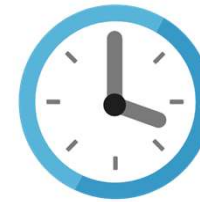
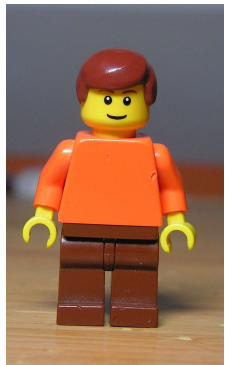
```
graph TD; A[Zero Trust] --- B[Verify Explicitly]; A --- C[JIT & JEA]; A --- D[Assume Breach];
```

Verify  
Explicitly

JIT & JEA

Assume  
Breach

# What?

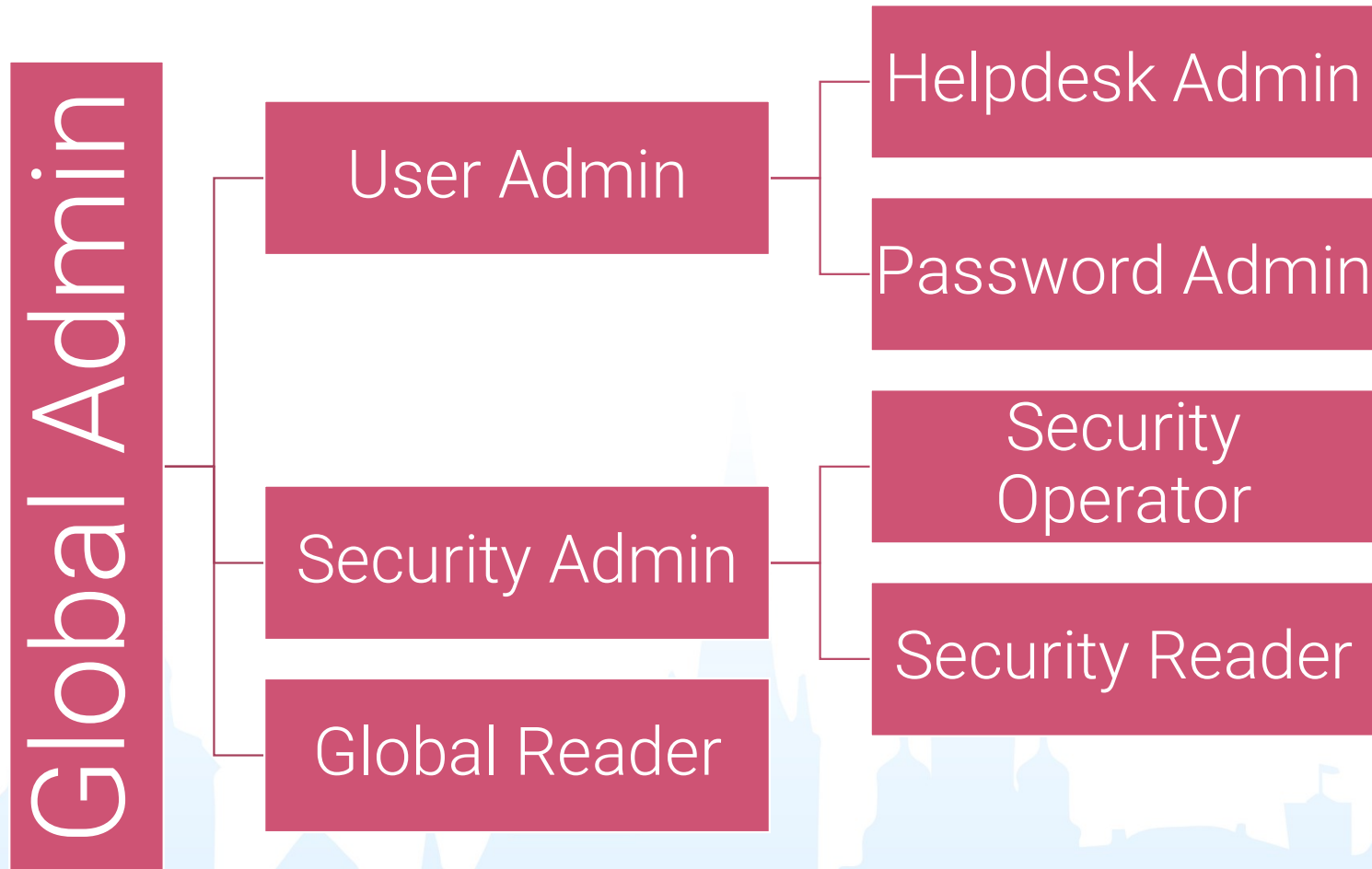


# Some 'uh-oh's to avoid

- Global Admin
- Privileged Role Administrator
- User Administrator
- Security Administrator
- Compliance Administrator

# Too many cooks?

Knowing the many layers of admin- rights

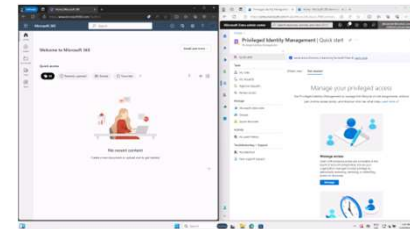


# Demo: JIT & JEA

Fortytwo  
BY AMESTO

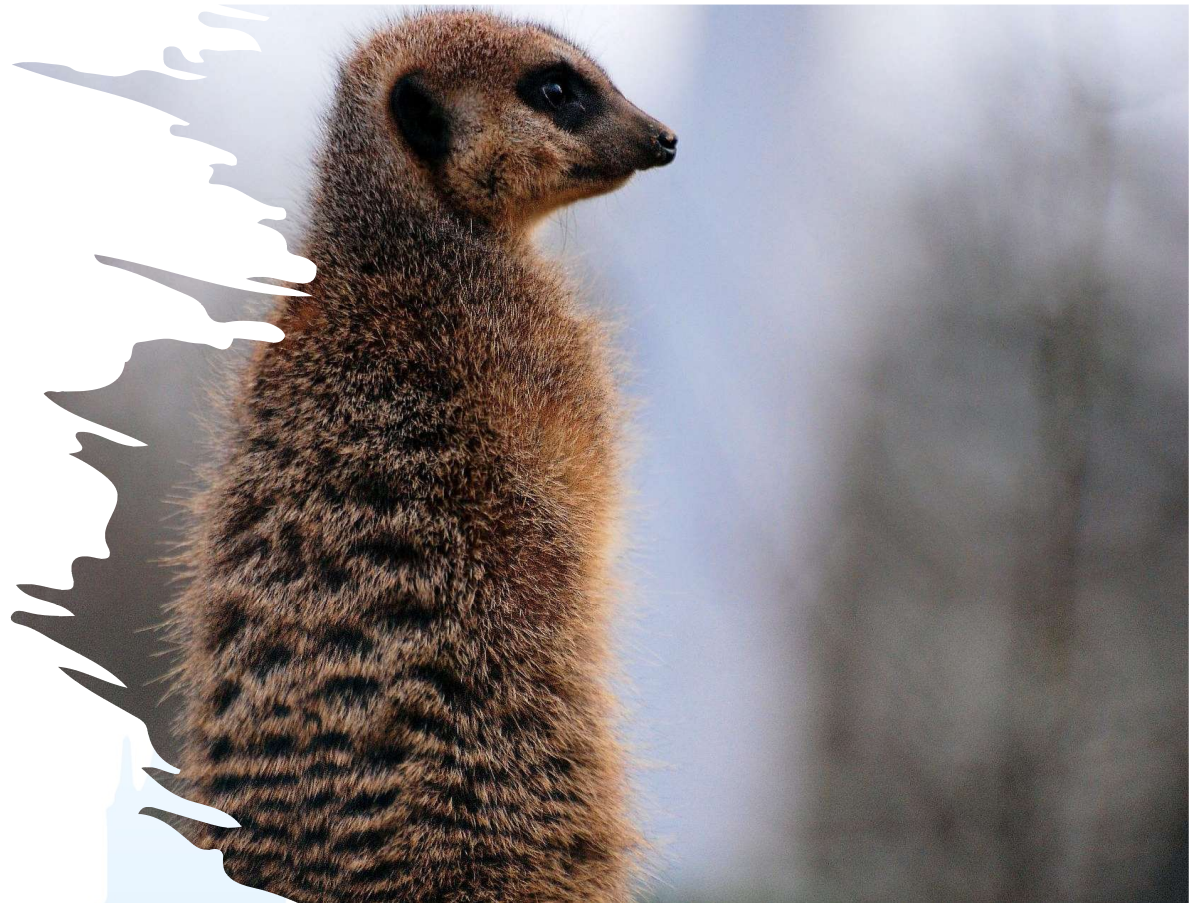


## DEMO TIME



# The watchguard

- Sign-ins logs
- News in Threats
- New features
- Those who still haven't enabled MFA



# Demo: MFA register and Conditional Access

**Fortytwo**  
BY AMESTO

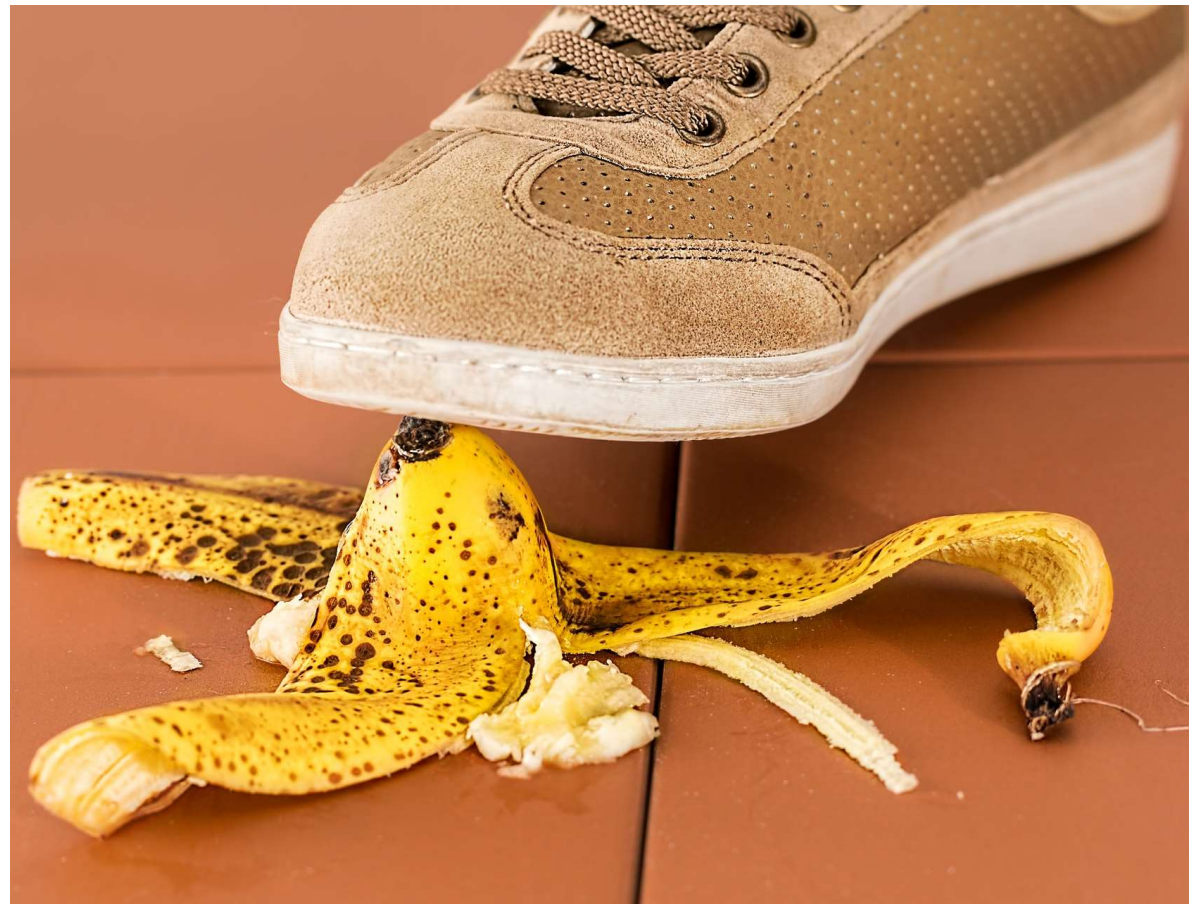


## DEMO TIME



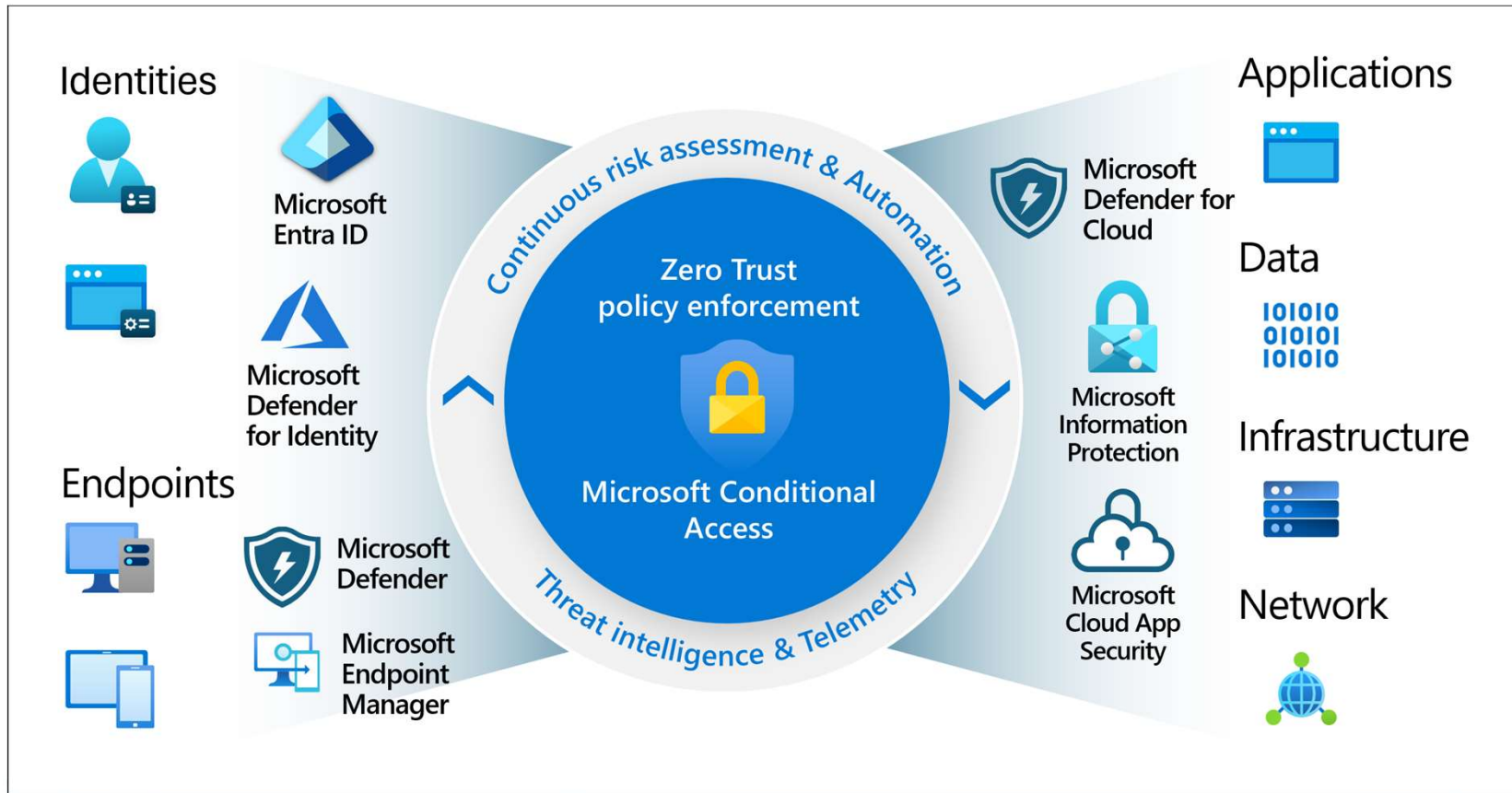
## ABSI in practice

- Sign-in risk
- User risk
- Impossible travel
- Trends
- Threats

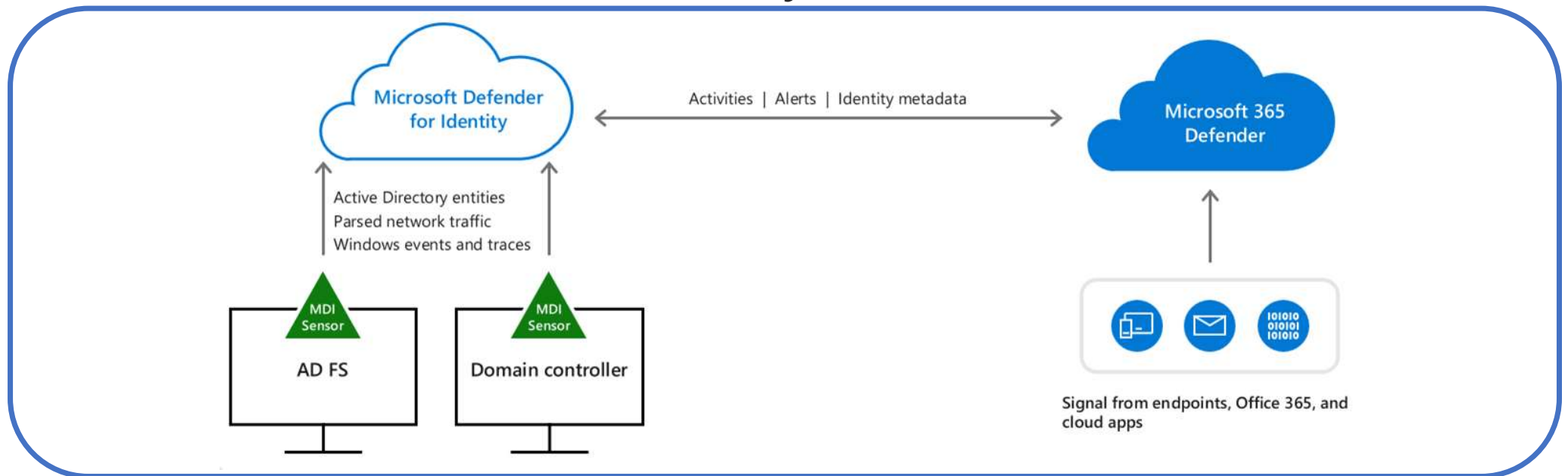




# What say thee, O' Microsoft?



# Microsoft Defender for Identity



- Monitor users, entity behavior, and activities with learning-based analytics
- Protect user identities and credentials stored in Active Directory
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
- Provide clear incident information on a simple timeline for fast triage

## Log into Defender for Identity:

<https://security.microsoft.com/settings/identities>

# Licensing for Identity Protection

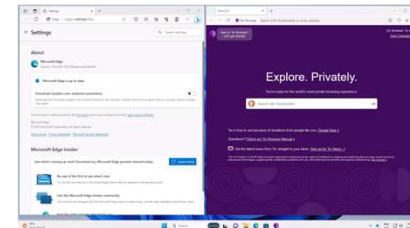
Capability		Microsoft Entra ID Free/ Microsoft 365 Apps	Microsoft Entra ID Premium P1	Microsoft Entra ID Premium P2
User risk policy (via Identity Protection)		No	No	Yes
Sign-in risk policy (via identity protection)		No	No	Yes
Security reports	Overview	No	No	Yes
	Risky users	Limited Information. *	Limited Information.*	Full access
	Risky sign-ins	Limited Information. *	Limited Information. *	Full access
	Risk detection	No	Limited Information. *	Full access
Notifications	User at risk alert	No	No	Yes
	Weekly digest	No	No	Yes
MFA registration policy		No	No	Yes

# Demo: Sign-in risk

Fortytwo  
BY AMESTO



## DEMO TIME



# Real-world scenario



[Support Escalation][Conditional Access][2306120050001449]



**Roberth Strand** <roberth@: .no>  
Til



tir. 13.06.2023 13:47

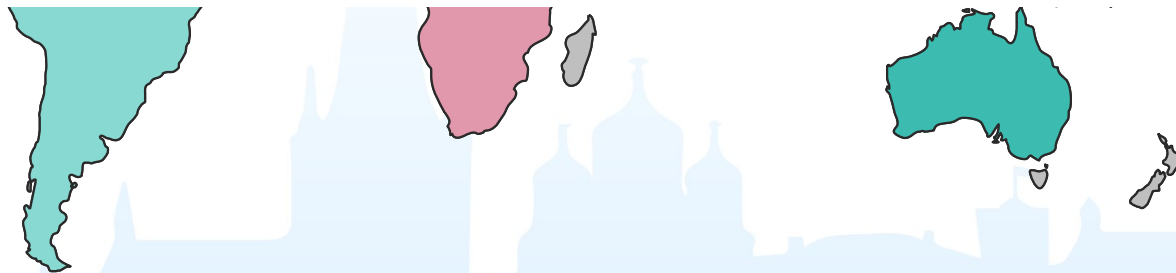
We have a customer who has managed to block all users from signing in. We have had a ticket open Monday morning, and we still haven't received any help from Microsoft support. From a partner standpoint, we have tried all other means to get around the conditional access policy, but nothing has worked.

They have been locked out for a while now, can we please get this escalated ASAP?

## **Roberth Strand**

Principal Cloud Engineer, **Amesto Fortytwo**

[LinkedIn](#) | [Mastodon](#) | [Twitter](#) | [Blog](#) | [Certifications](#)



# Demo: Secure score

**Fortytwo**  
BY AMESTO

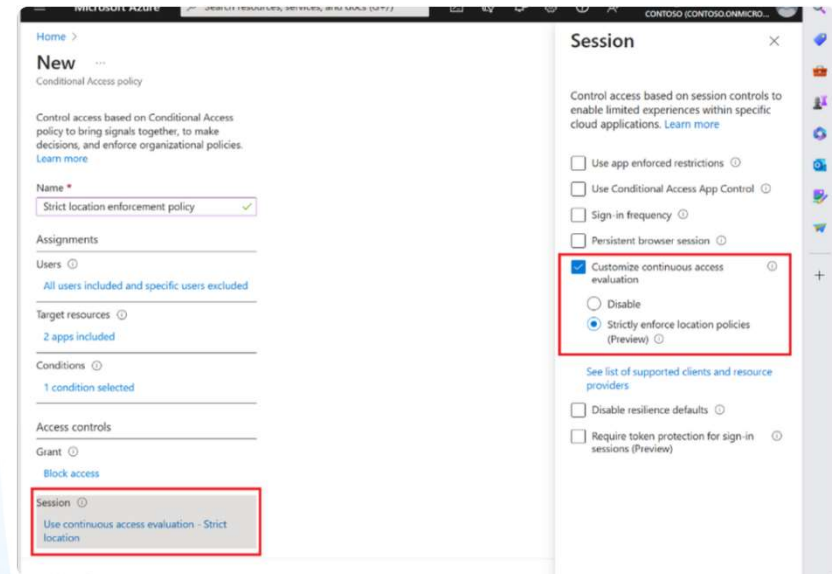


## DEMO TIME



# Wait – there is more!

## Strictly Enforce Location Policies with Continuous Access Evaluation





# Please rate this session!

Your feedback will help with

- speaker evaluation
- content relevance
- decision making for future events
- quality improvement
- ...and saving Alex's butt!



# Thank you!

# Q&A

