

#ScottishSummit2023

Saving Your Butt:

The many layers of Identity Protection

Alexander Solaat Rødland & Olav Tvedt
Amesto Fortytwo & Sparebanken Vest





Thank You to our Sponsors...

Silver Sponsors

PROMX

DOCENTRIC

conspicuous

dox42[®]
automate your documents
integrate your data

māzīkglobal

ANS

Online Sponsor

knk

Lunch Sponsor

PROXIMO

data8
The Data Quality Company

Alexander Solaat Rødland

Principal Cloud Architect
Amesto Fortytwo



- Geek for more than 20 years
- Microsoft MVP – Windows and Devices for IT
- Windows Insider MVP
- This trip is my honeymoon(!)

“It’s easier to stay out, than get out”



<https://www.linkedin.com/in/alexsolaat/>



<https://solaat.no/>



alexsolaat



<https://www.youtube.com/@bluescreenbrothers>

#ScottishSummit2023

Olav Tvedt

Cloud Dude
Sparebanken Vest



- 16 x MVP Azure
- I know MS DOS!
- Alex did NOT bring me on his honeymoon

"I never LOSE, I either WIN or LEARN"



<https://www.linkedin.com/in/otvedt/>



<https://olavtvedt.blogspot.com/>



olavtwitt



<https://github.com/OTvedt/Scripts-For-Sharing>



<https://www.youtube.com/@bluescreenbrothers>



#ScottishSummit2023



Who are you?



#ScottishSummit2023



What are you accessing?



#ScottishSummit2023

Getting 'modern'



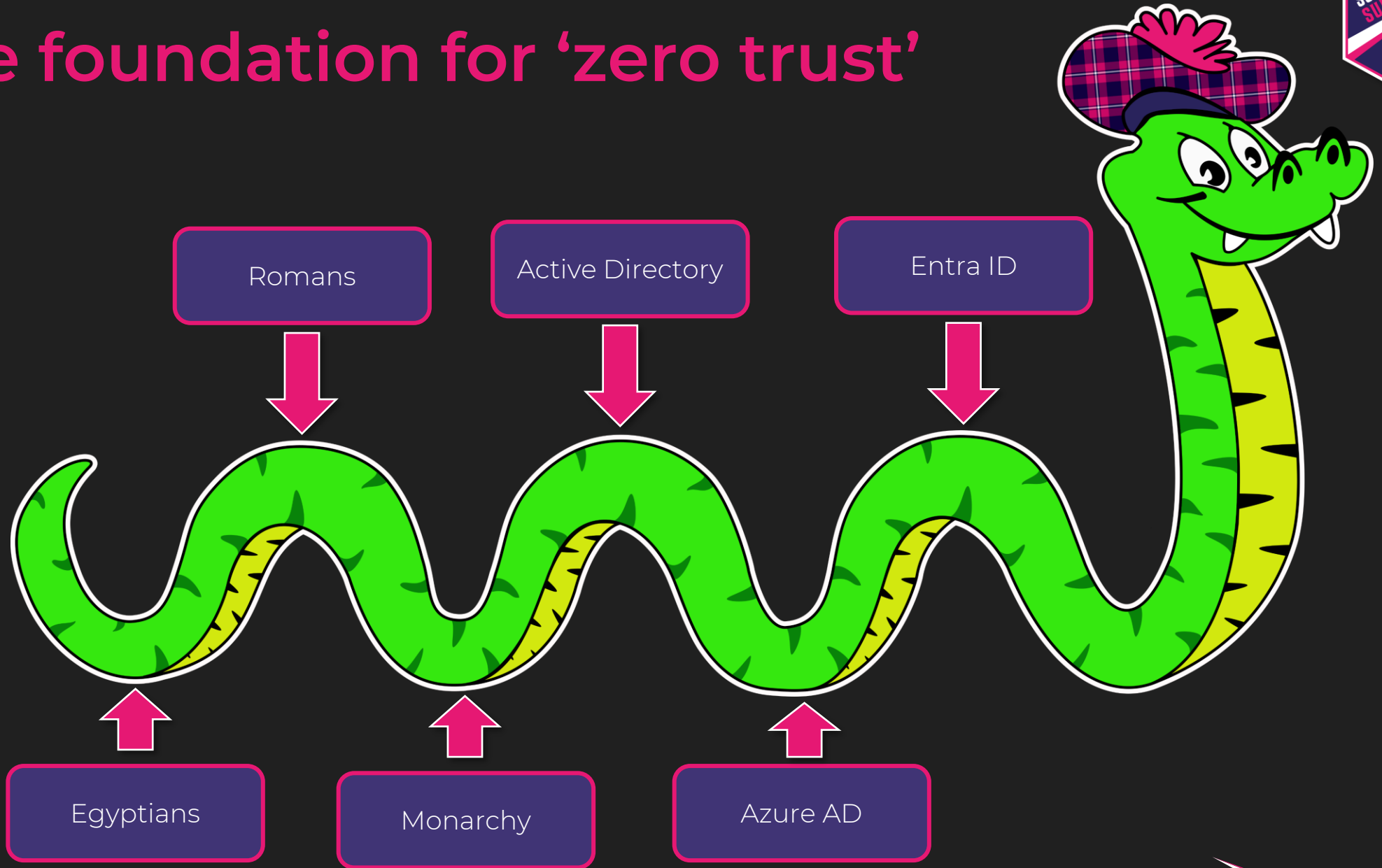
Where is Waldo?

- Any calls from «Microsoft» lately?





The foundation for 'zero trust'



ABSI (Artificial Butt-Saving Intelligence)

- Block identity takeover in real-time



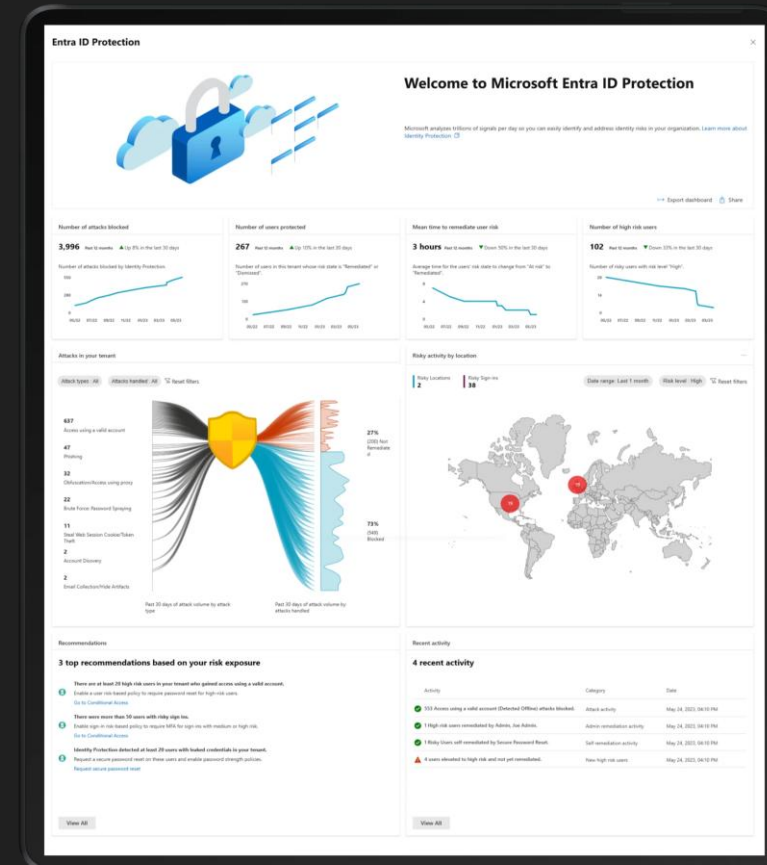
Prevent identity compromise



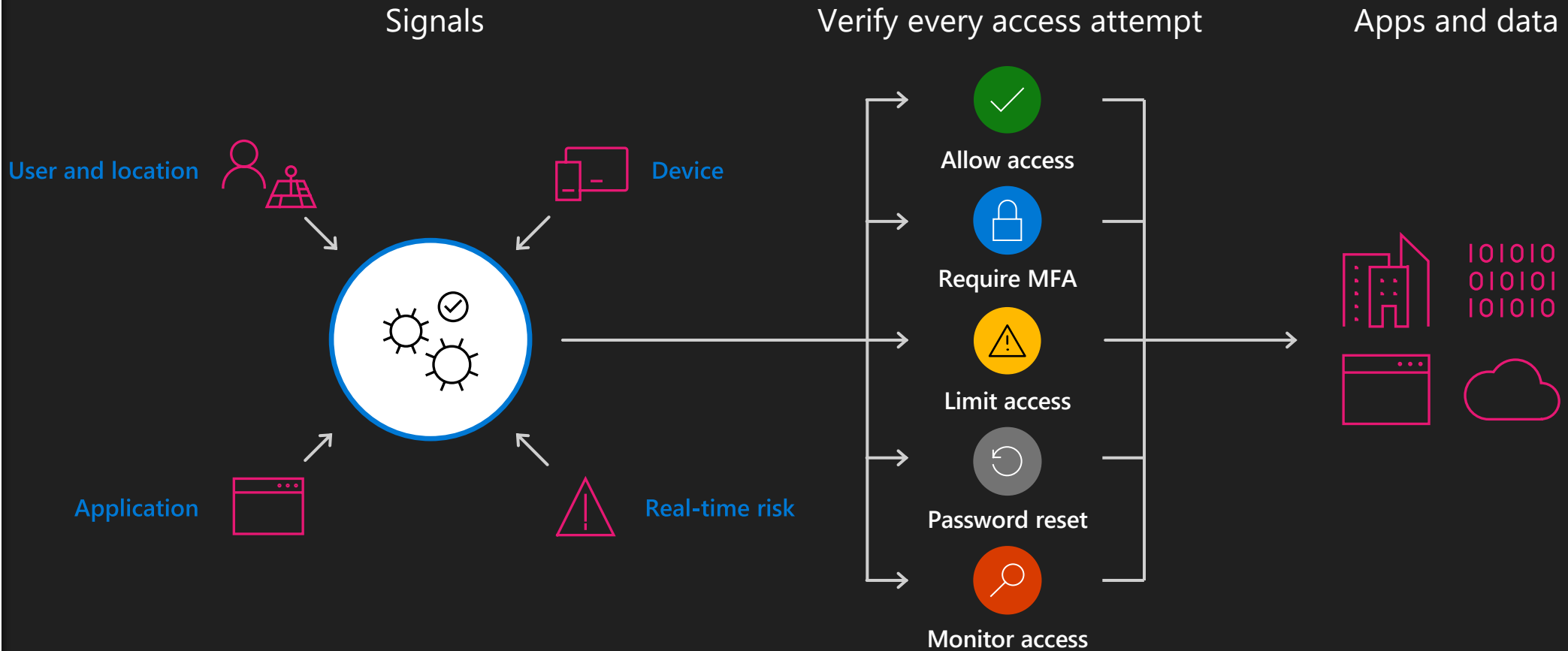
Enforce policies



Seamlessly integrate



40TB of butt-saving security signals



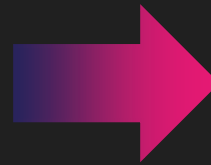
- Azure AD

Azure AD Free

Azure AD Premium P1

Azure AD Premium P2

Azure AD External Identities



- Microsoft Entra ID

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

Microsoft Entra External ID



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

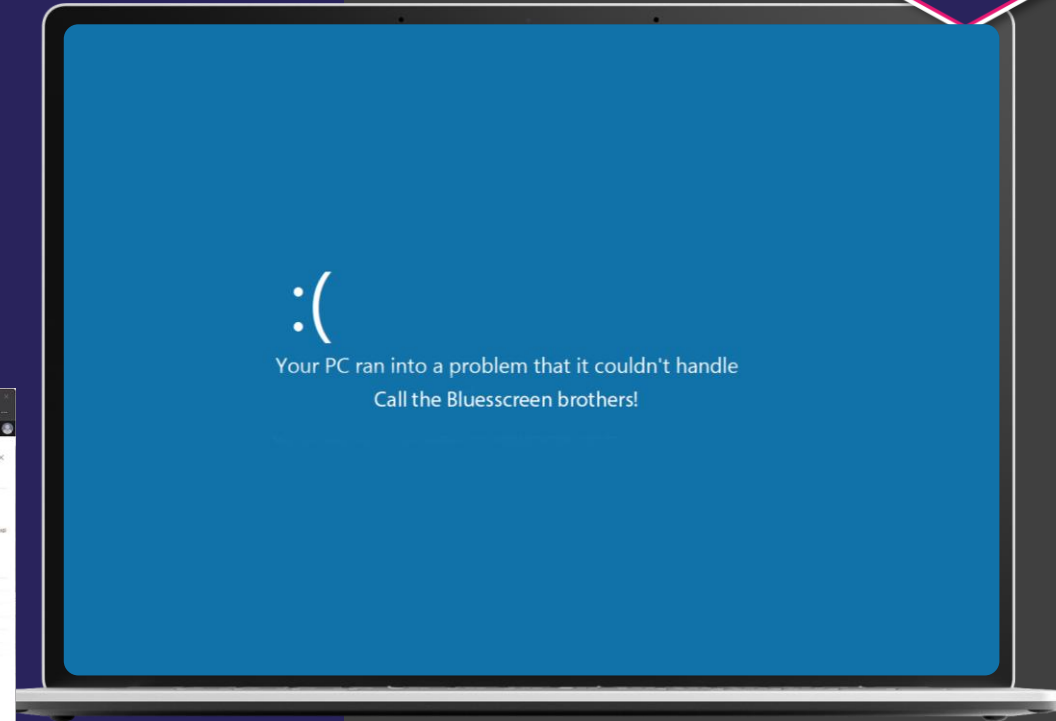
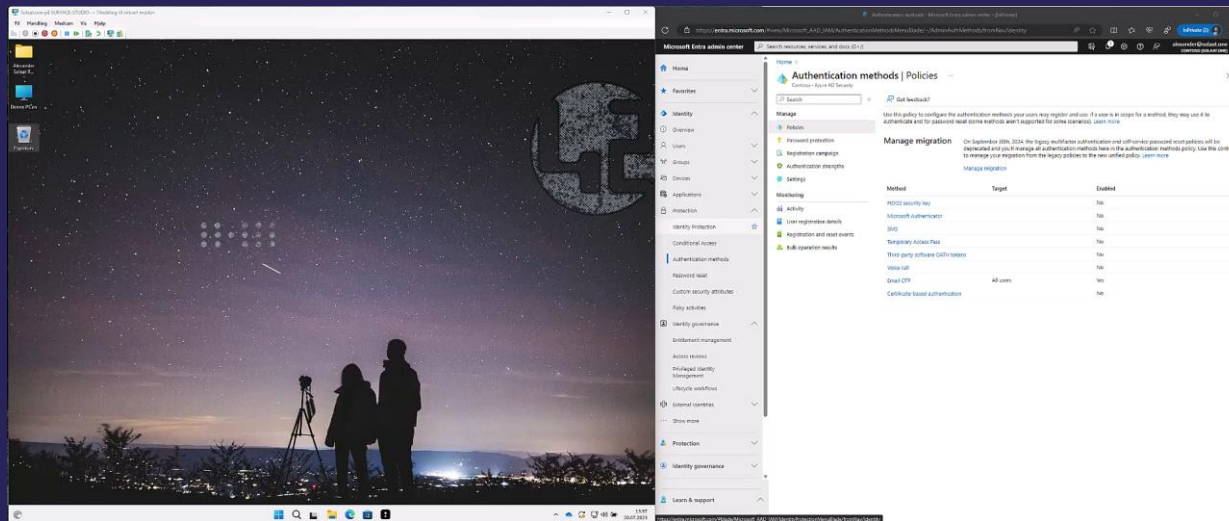
Enforce key restrictions Yes No

Restrict specific keys Allow Block

[Add AAGUID](#)

No AAGUIDs have been added.

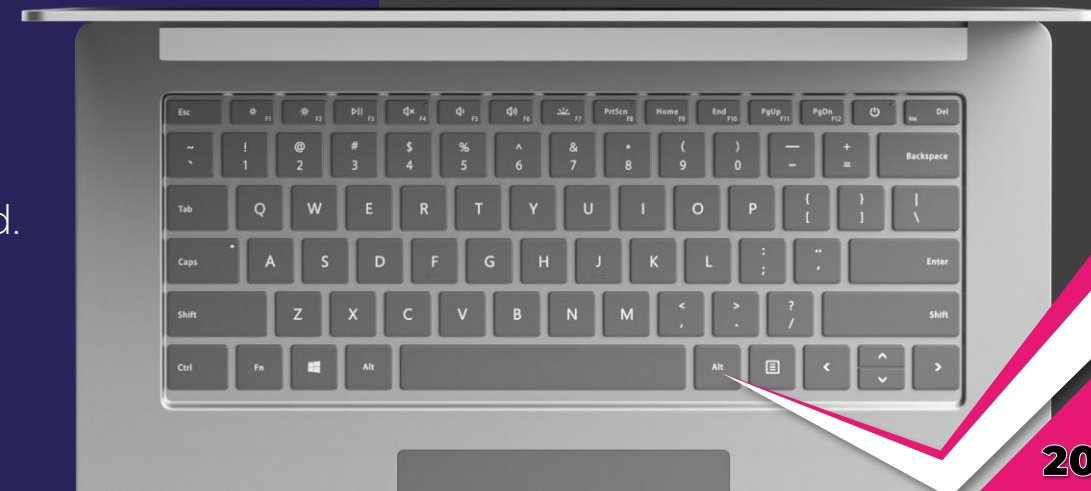
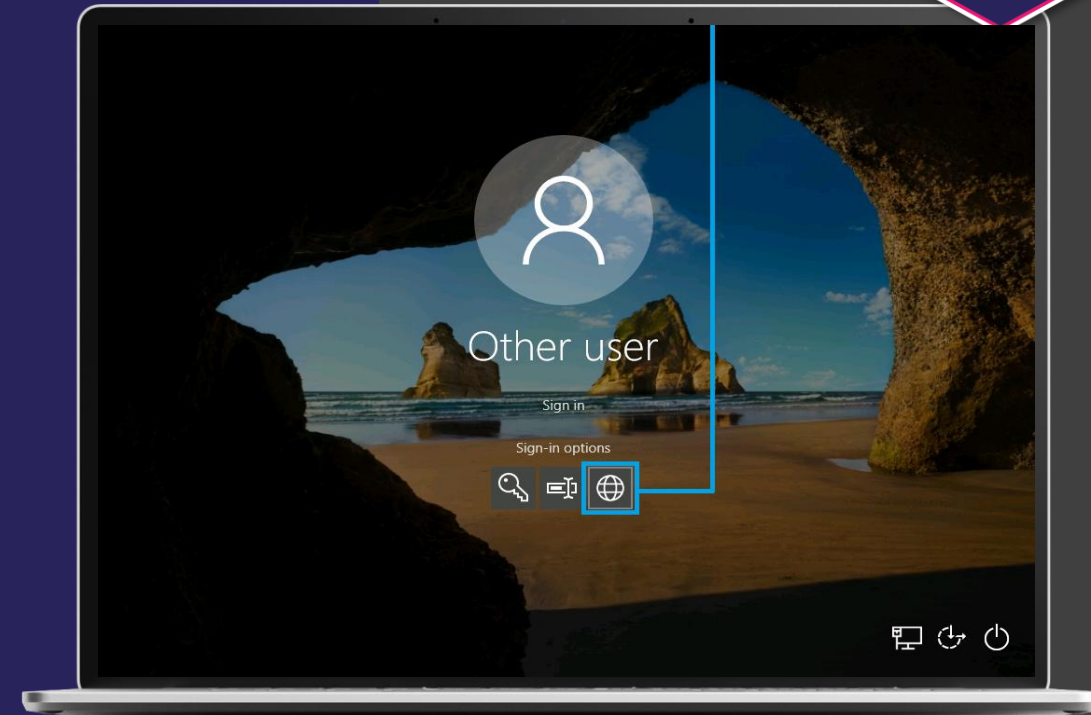
Demo: TAP



TAP

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.



P@\$\$w0rd?





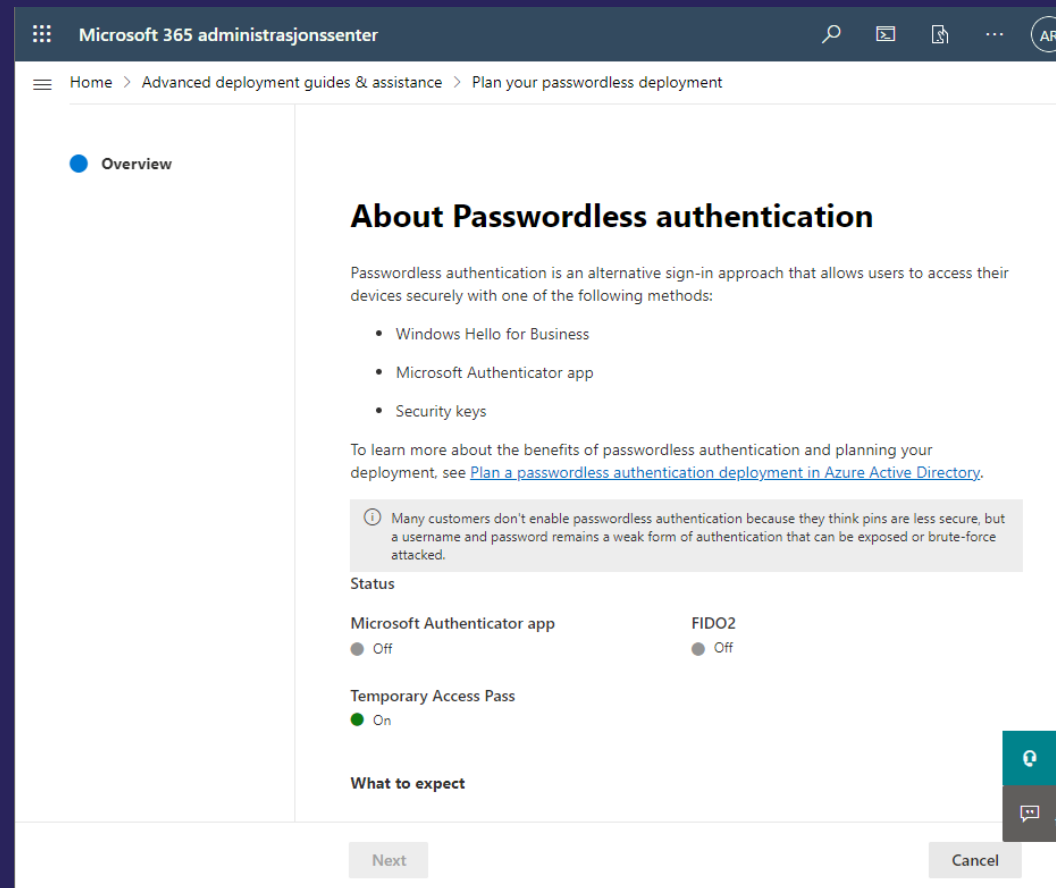
Hello vs Hello for Business

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

Go passwordless

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

A screenshot of the Microsoft 365 Admin Center interface. The page title is "Plan your passwordless deployment". The main heading is "About Passwordless authentication". The text explains that passwordless authentication is an alternative sign-in approach and lists three methods: Windows Hello for Business, Microsoft Authenticator app, and Security keys. A note states that many customers don't enable passwordless authentication because they think pins are less secure. The "Status" section shows "Microsoft Authenticator app" and "FIDO2" are both "Off", while "Temporary Access Pass" is "On". There are "Next" and "Cancel" buttons at the bottom.

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

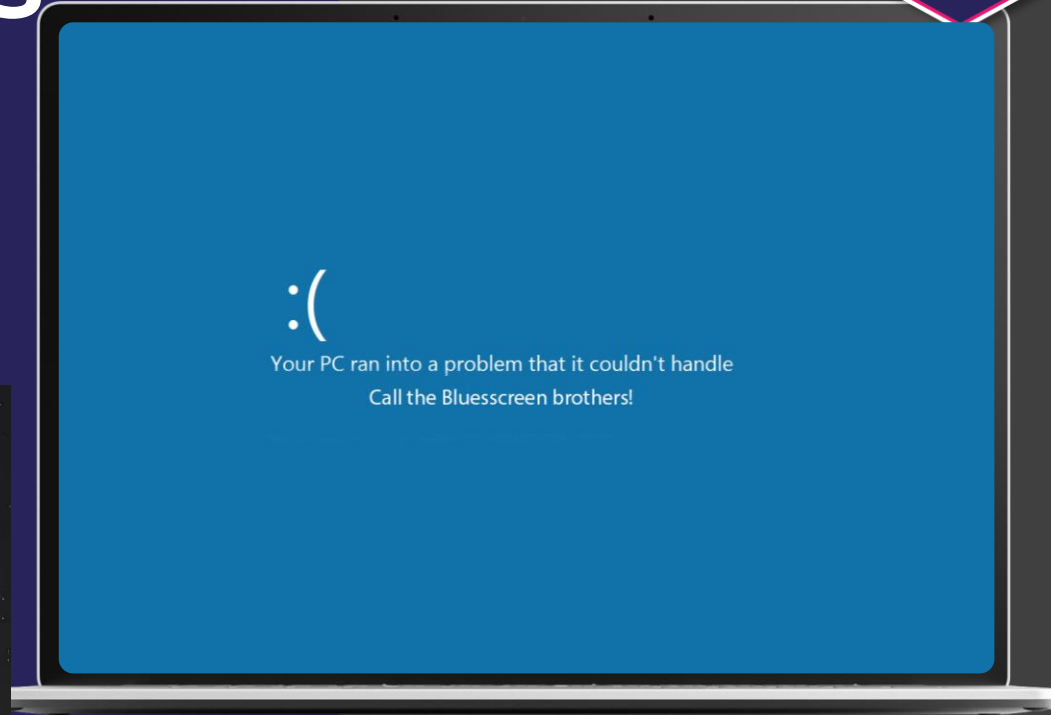
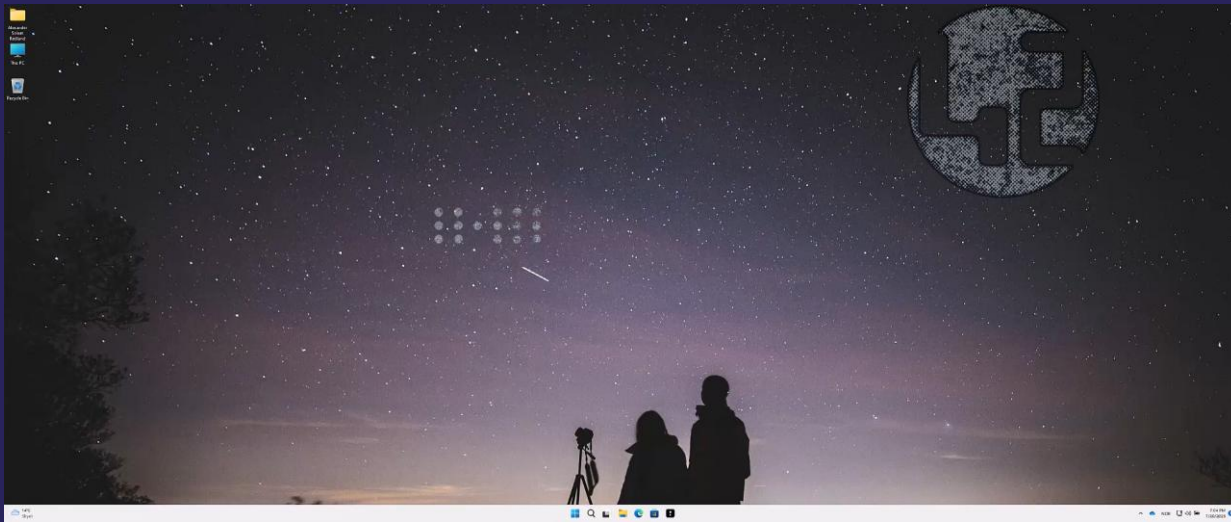
FIDO2 Off

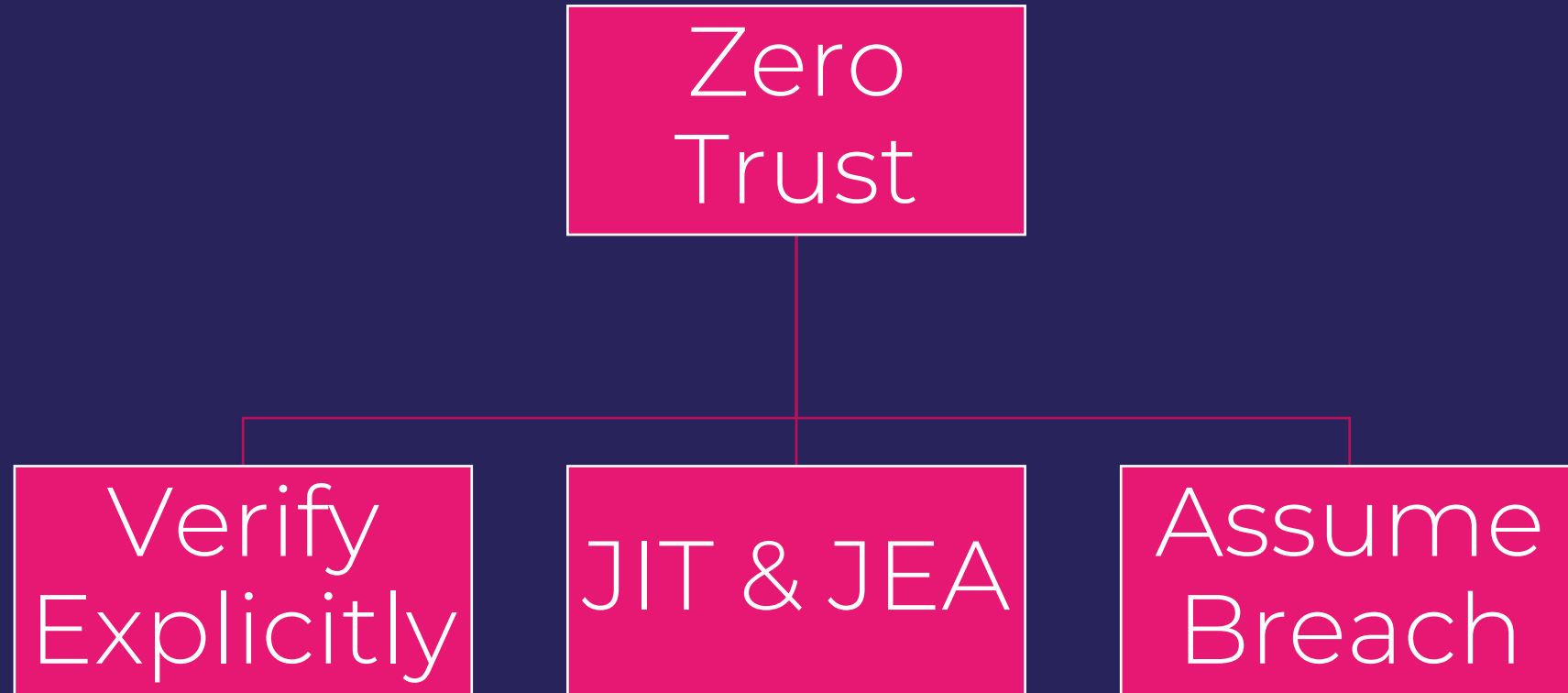
Temporary Access Pass On

What to expect

Next Cancel

Demo: Passwordless





What?





Some 'uh-oh's to avoid

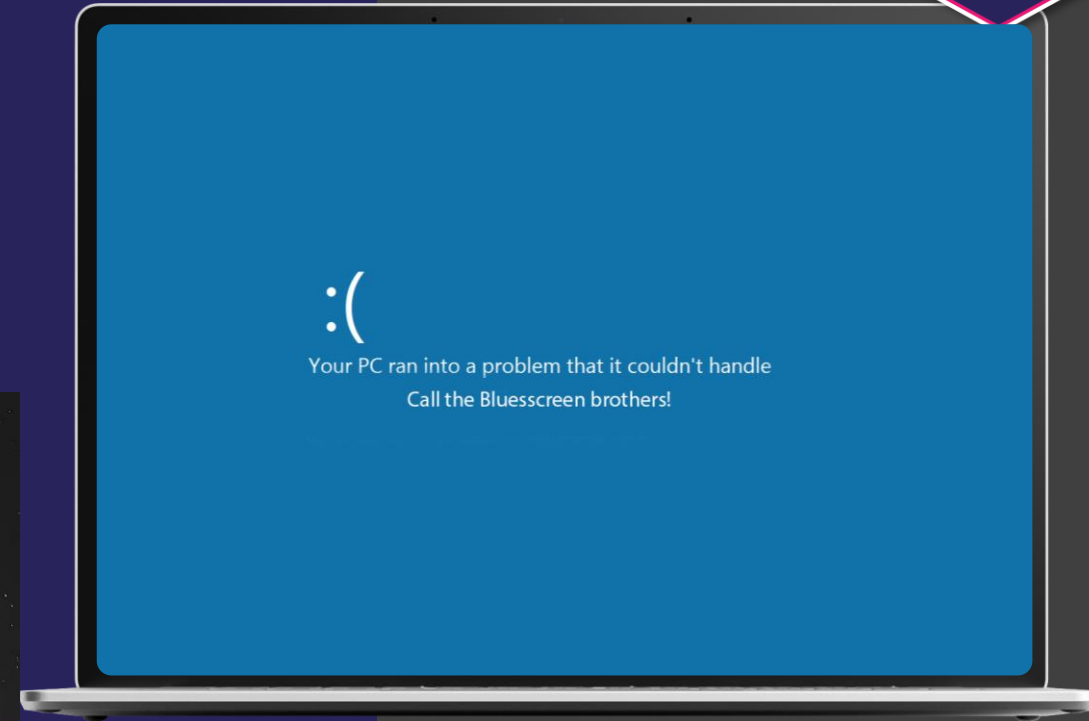
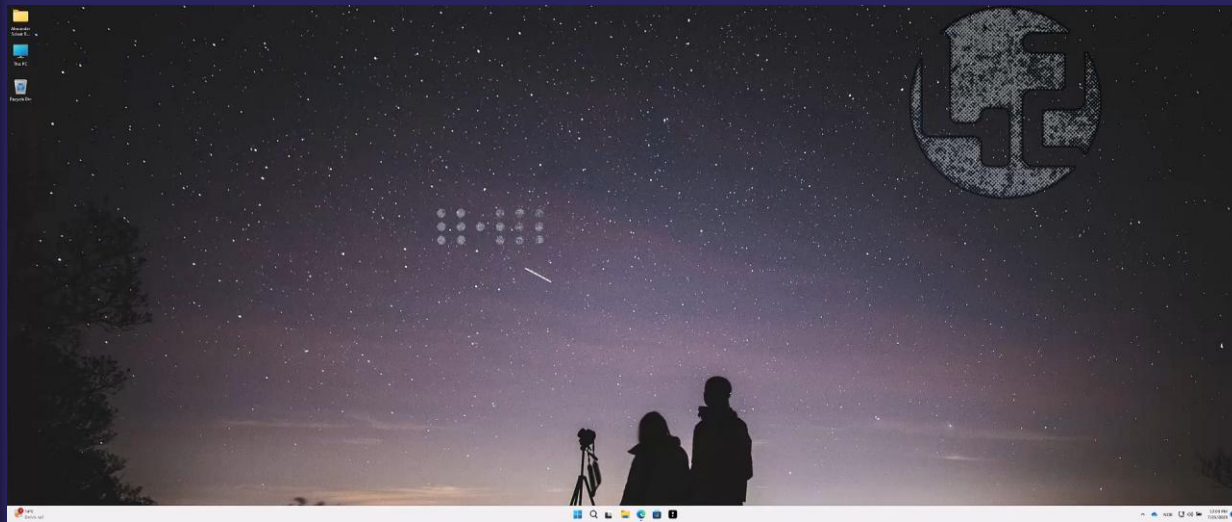
- Global Admin
- Privileged Role Administrator
- User Administrator
- Security Administrator
- Compliance Administrator



What about Azure?



Demo: JIT & JEA

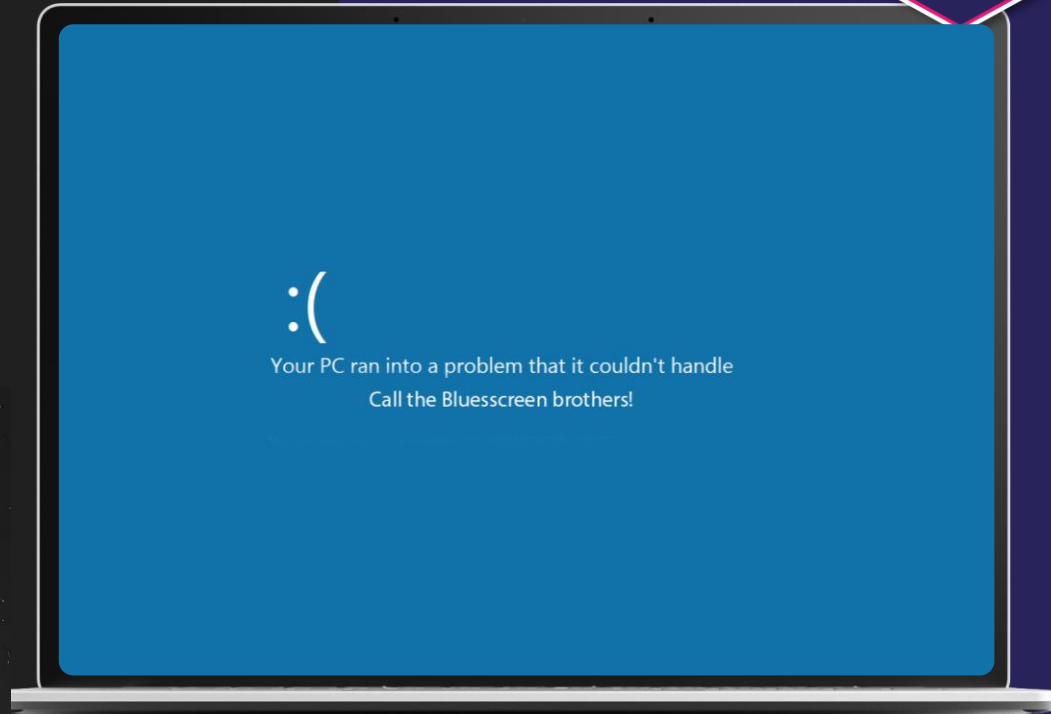
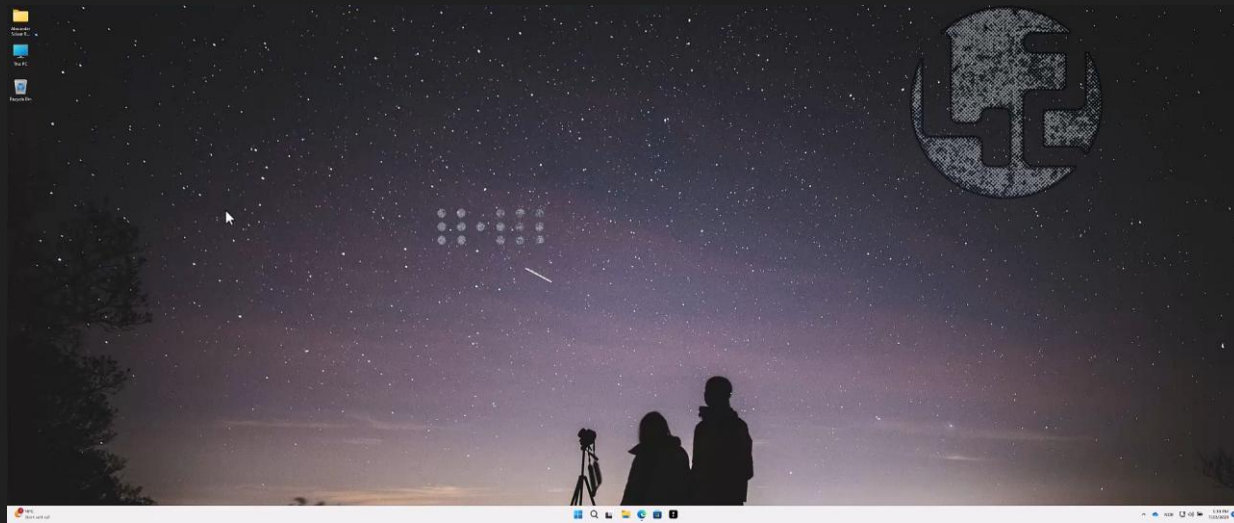


The watchguard

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



Demo: MFA register and Conditional Access

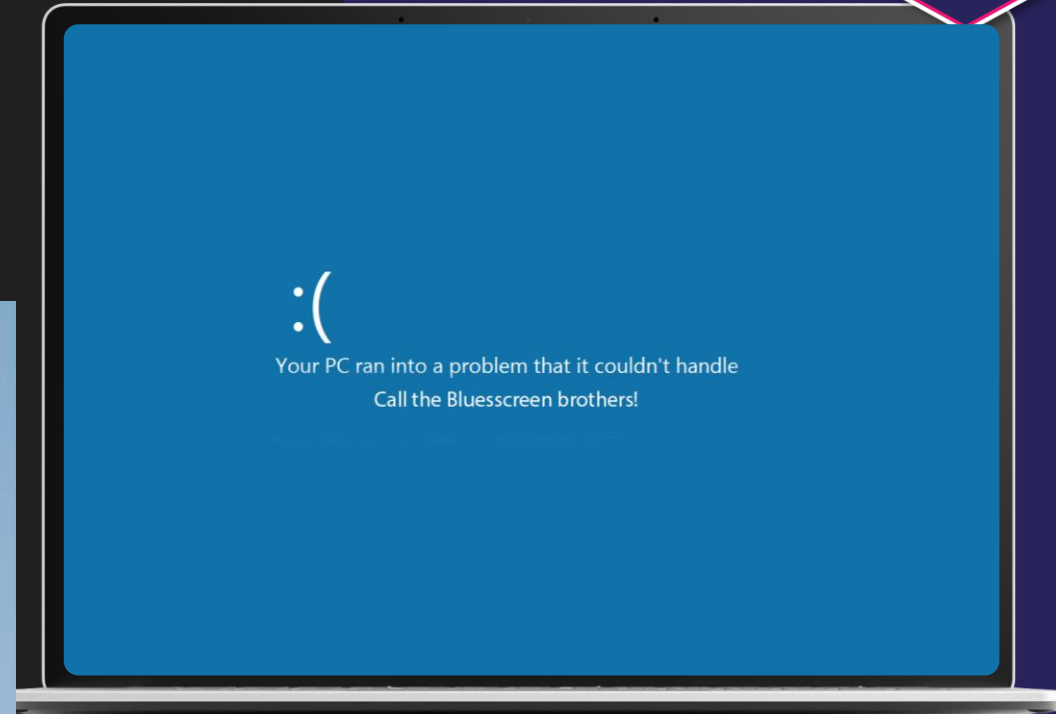
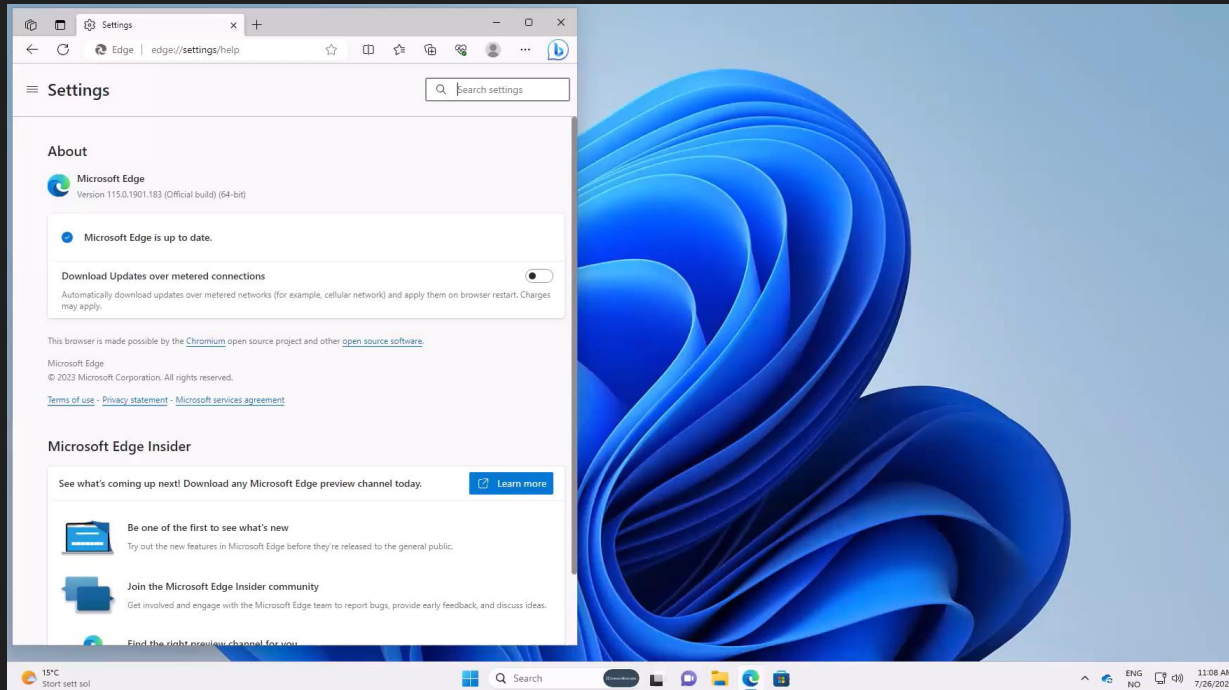


ABSI in practice

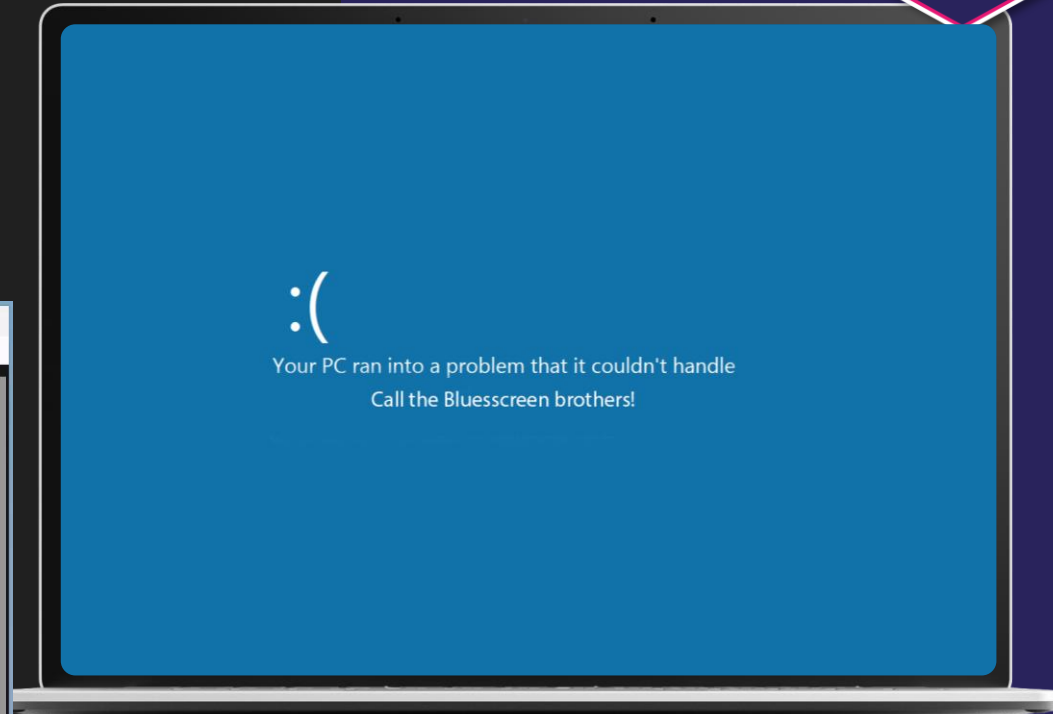
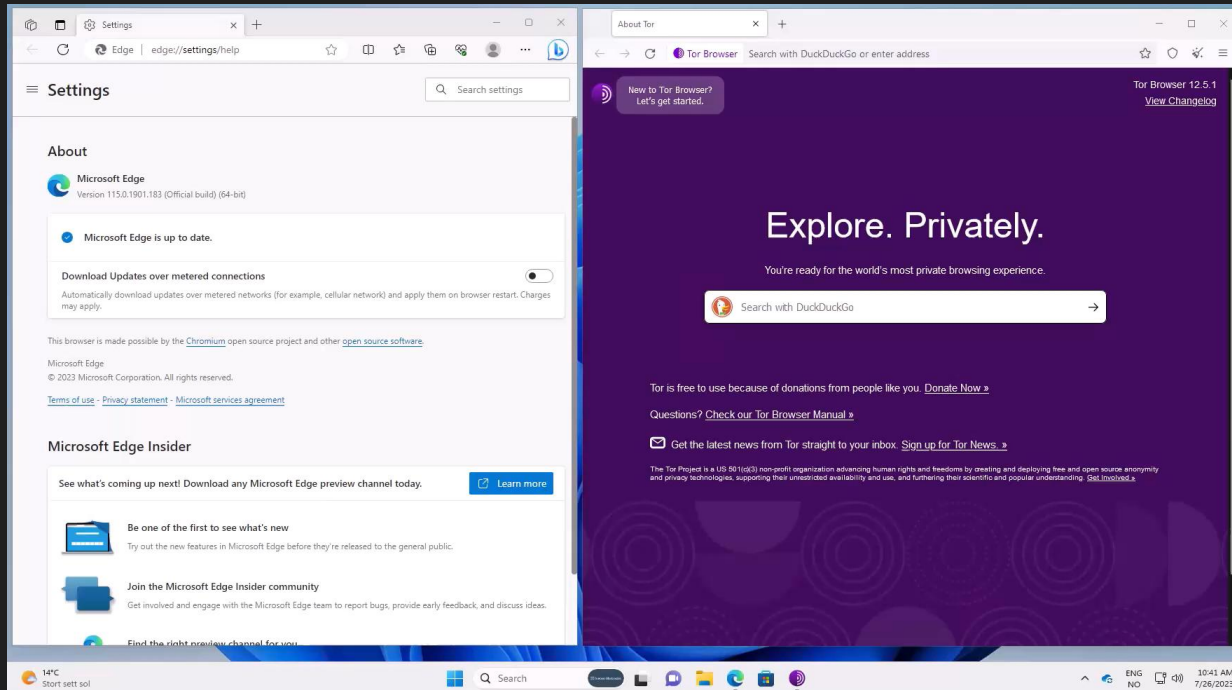
- Sign-in risk
- User risk
- Impossible travel
- Trends
- Threats



Demo: User risk



Demo: Sign-in risk



Real-world scenario

[Support Escalation][Conditional Access][2306120050001449]



Roberth Strand <roberth@[redacted].no>
Til [redacted]



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](#)

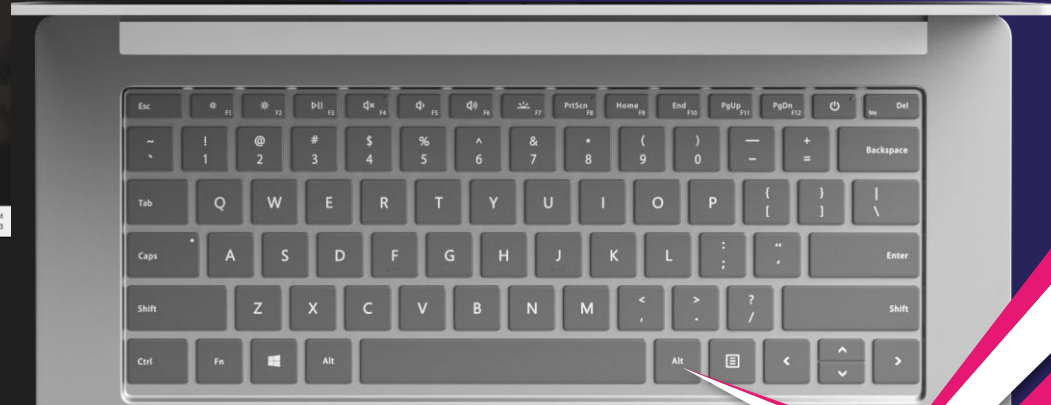
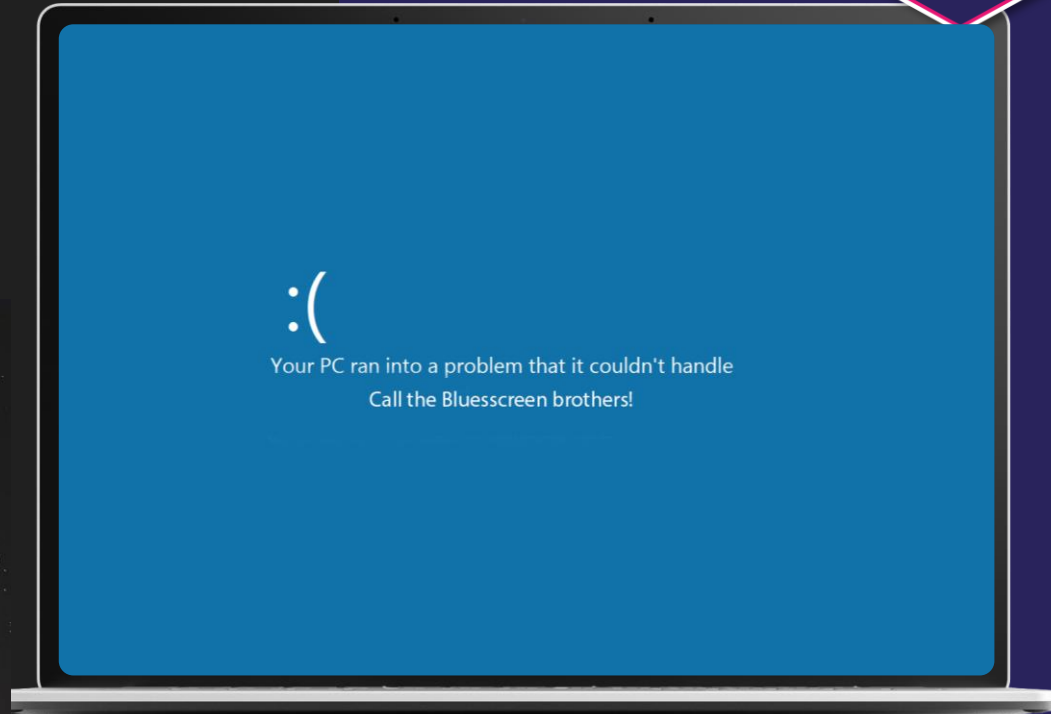
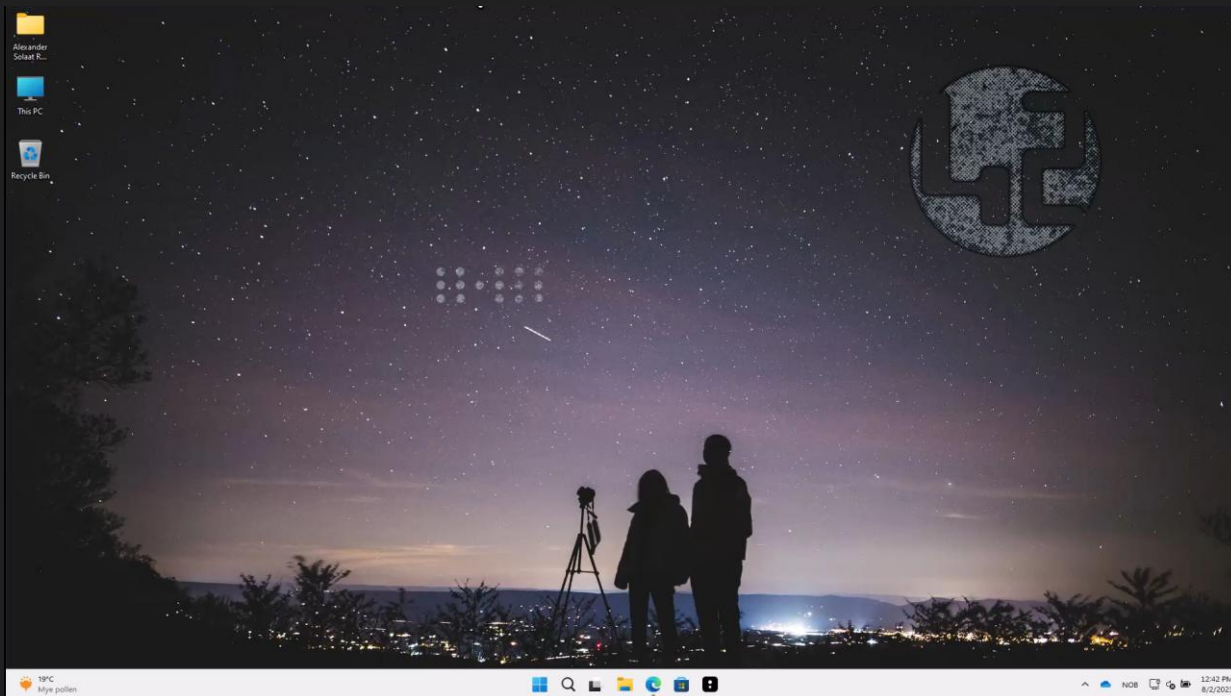
What is our score?

Things change, so do you!




FOTO: FREDRIK VARFJELL / NTB

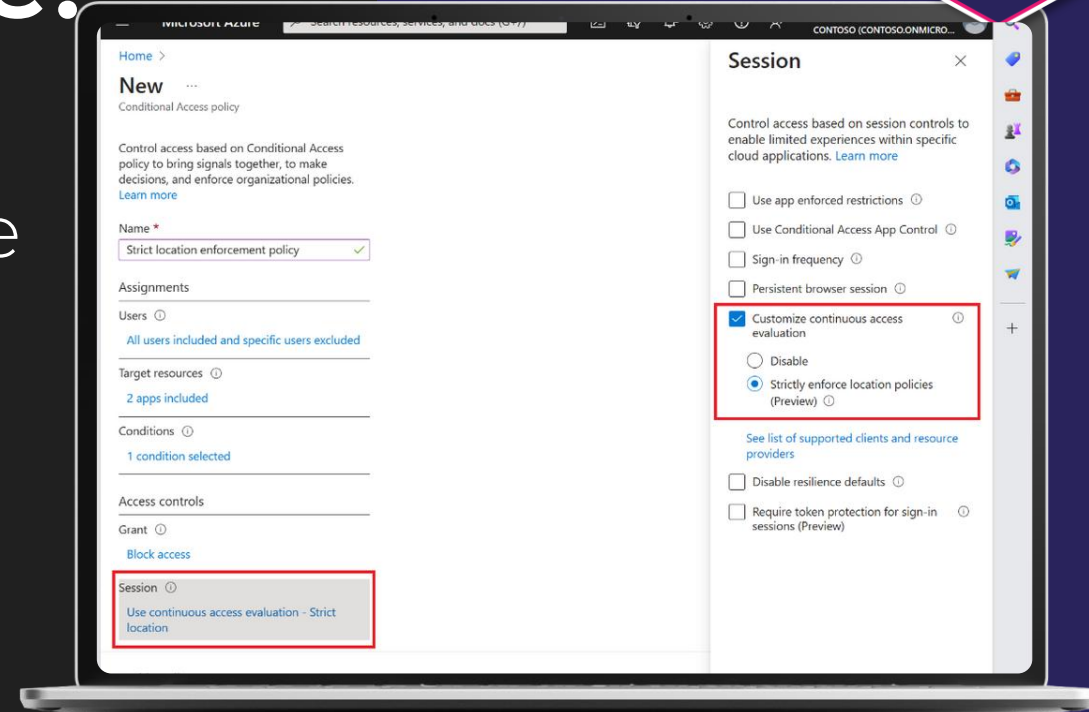
Demo: Secure score



Wait – there is more!

- Public Preview: Strictly Enforce Location Policies with Continuous Access Evaluation

By  [Alex Weinert](#)
Published Jul 28 2023 10:15 AM





Save our butts!

“We rise by uplifting others”



#ScottishSummit2023