

Securing your Digital Workspace: Best Practices for Protecting your Microsoft 365 from Cyber Threats

Friday November 3rd, 2023

12:30-1:40pm EST



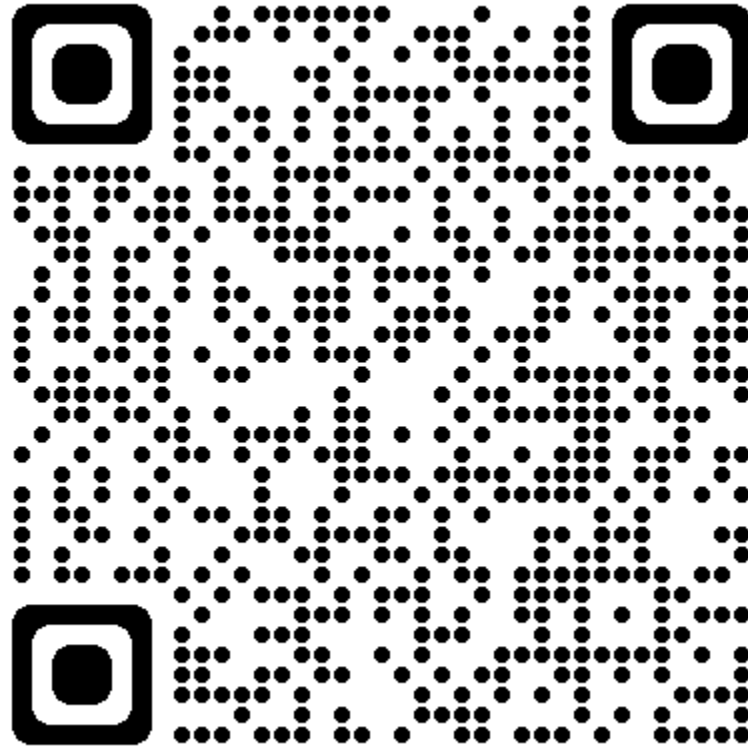
Introductions: Peter Carson



- President, Envision IT and Extranet User Manager
- 13-time Office Apps and Services Microsoft MVP
- peter@envisionit.com
- blog.petercarson.ca
- www.envisionit.com
- www.extranetusermanager.com
- President, Toronto SharePoint User Group



Presentation Download



Agenda

- Identity Fundamentals
- Security
- Where do standalone communication and Team Sites fit in?
- Guests versus B2B Direct Connect
- Open-Source Solutions for analyzing and optimizing your IA
- Summary, Q&A and Closing

Session Overview and Goals

Entra ID is the
core security
infrastructure

Features depend
on licenses

Many other
Microsoft
products are part

Balancing security
and UX is key

Apply the right
security to the
right sensitivity

Factor in internal
and external users

Discover the Microsoft Entra product family



Entra ID

Safeguard your organization with the identity and access management solution that connects people to their apps, devices, and data.



Microsoft Entra Permissions Management

Discover, remediate, and monitor permission risks across your multicloud infrastructure with a cloud infrastructure entitlement management (CIEM) solution.



Microsoft Entra Verified ID

Create, issue, and verify privacy-respecting decentralized identity credentials with an identity verification solution that helps you enable more secure interactions with anyone or anything.

[Microsoft Entra - Secure Identities and Access | Microsoft Security](#)

Entra ID Versions

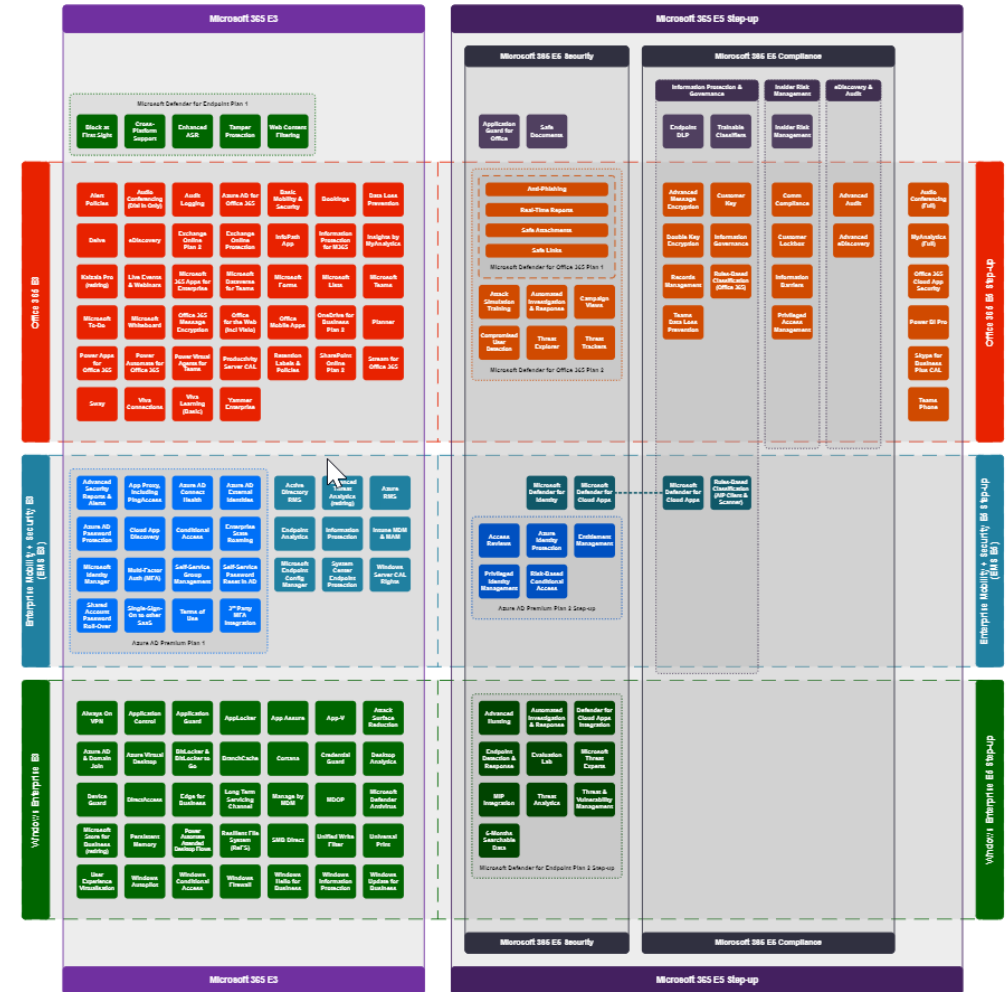
		Most comprehensive	Promotional offer available ²
Microsoft Entra ID Free	Microsoft Entra ID P1	Microsoft Entra ID P2	Microsoft Entra ID Governance
Free	\$6.00 user/month	\$9.00 user/month	\$7.00 user/month
Included with Microsoft cloud subscriptions such as Microsoft Azure, Microsoft 365, and others. ¹	Microsoft Entra ID P1 (formerly Azure Active Directory P1) is available as a standalone or included with Microsoft 365 E3 for enterprise customers and Microsoft 365 Business Premium for small to medium businesses.	Microsoft Entra ID P2 (formerly Azure Active Directory P2) is available as a standalone or included with Microsoft 365 E5 for enterprise customers.	Entra ID Governance is an advanced set of identity governance capabilities for Microsoft Entra ID P1 and P2 customers. Special pricing is available for Microsoft Entra P2 customers.

[Microsoft Entra Plans and Pricing | Microsoft Security](#)

Microsoft 365 Licensing

Aaron Dinnage

- <https://m365maps.com>
- <https://github.com/AaronDinnage/Licensing>
- Maps for many different product combinations



Updates to Azure AD External Identity Licensing

- Only applies to Azure AD Premium features
 - Free for all users if not using premium features
 - Staff also need to be licensed for the same Premium features
- Price based on Monthly Active Users (MAU)
 - Replaces 1:5 billing ratio

	Premium P1	Premium P2
First 50,000 MAU	\$0/Monthly Active Users	\$0/Monthly Active Users
More than 50,000 MAU	\$0.00416/Monthly Active Users	\$0.020800/Monthly Active Users

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-pricing>
<https://azure.microsoft.com/en-us/pricing/details/active-directory/external-identities/>

External Users in Microsoft 365

Microsoft Definition:

- “External Users means users that are not employees, onsite contractors or onsite agents of Customer or its Affiliates.”
 - Refer to [Commercial Licensing Terms \(microsoft.com\)](#)
- Internal employee users are not eligible
 - Consider [Microsoft 365 F1](#)

Types of Azure AD Users and Authentication

Member - Synced

- Synced from on premise Active Directory
- Authentication options
 - Password hash synchronization (PHS)
 - Pass-through authentication (PTA)
 - Federation

Member – Cloud Only

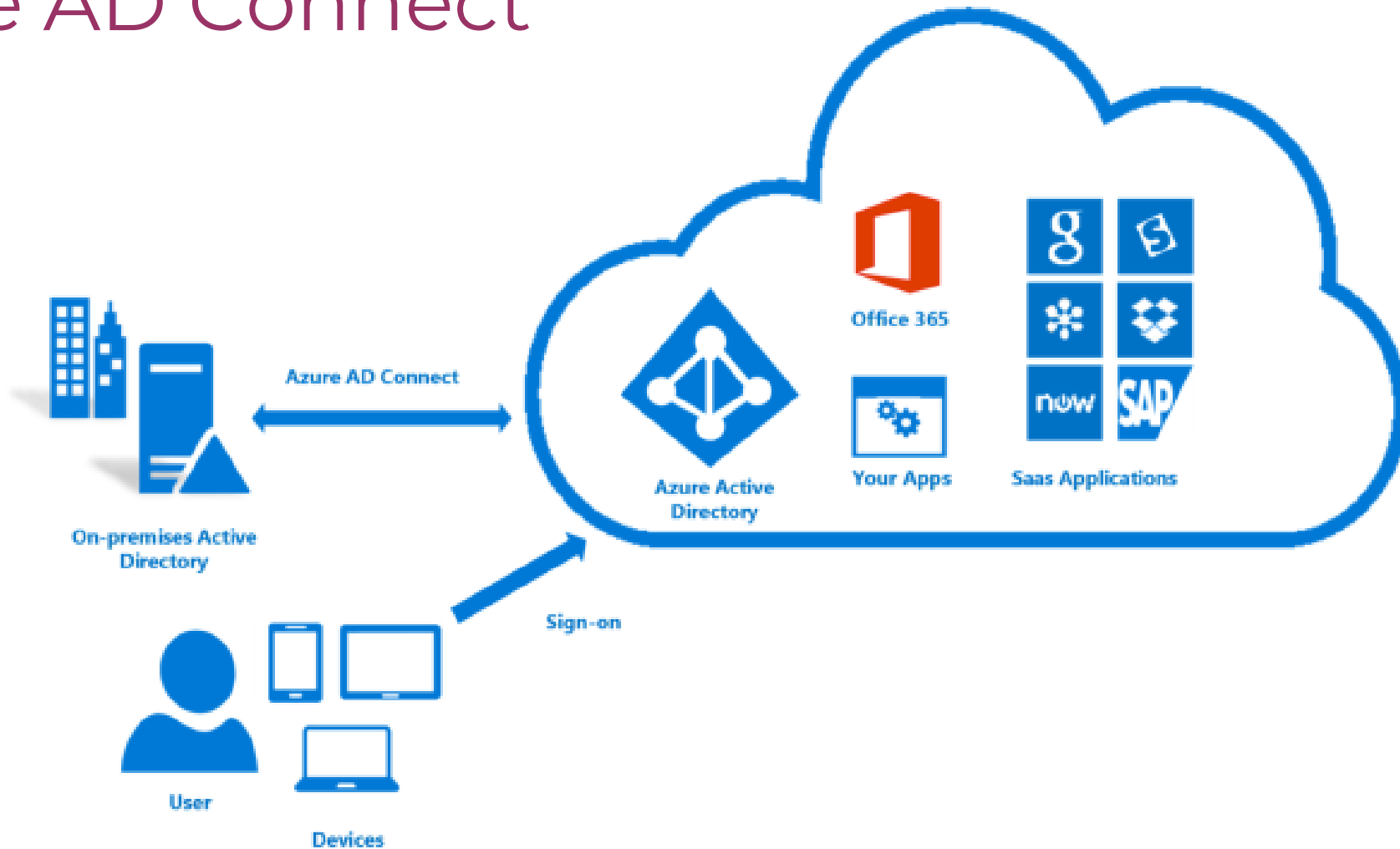
- Account only exists in the cloud
- Authentication options
 - Cloud password
 - Federation

Guest

- Invited in
 - Microsoft 365
 - Azure guest invitation
- Authentication Options
 - Their Microsoft organizational or personal credentials
 - Google, Facebook
 - Federation
 - One time passcode

[Azure AD Connect: User sign-in - Microsoft Entra | Microsoft Learn](#)

Azure AD Connect



<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect>

Azure AD Connect versus Connect Cloud Sync

Connect

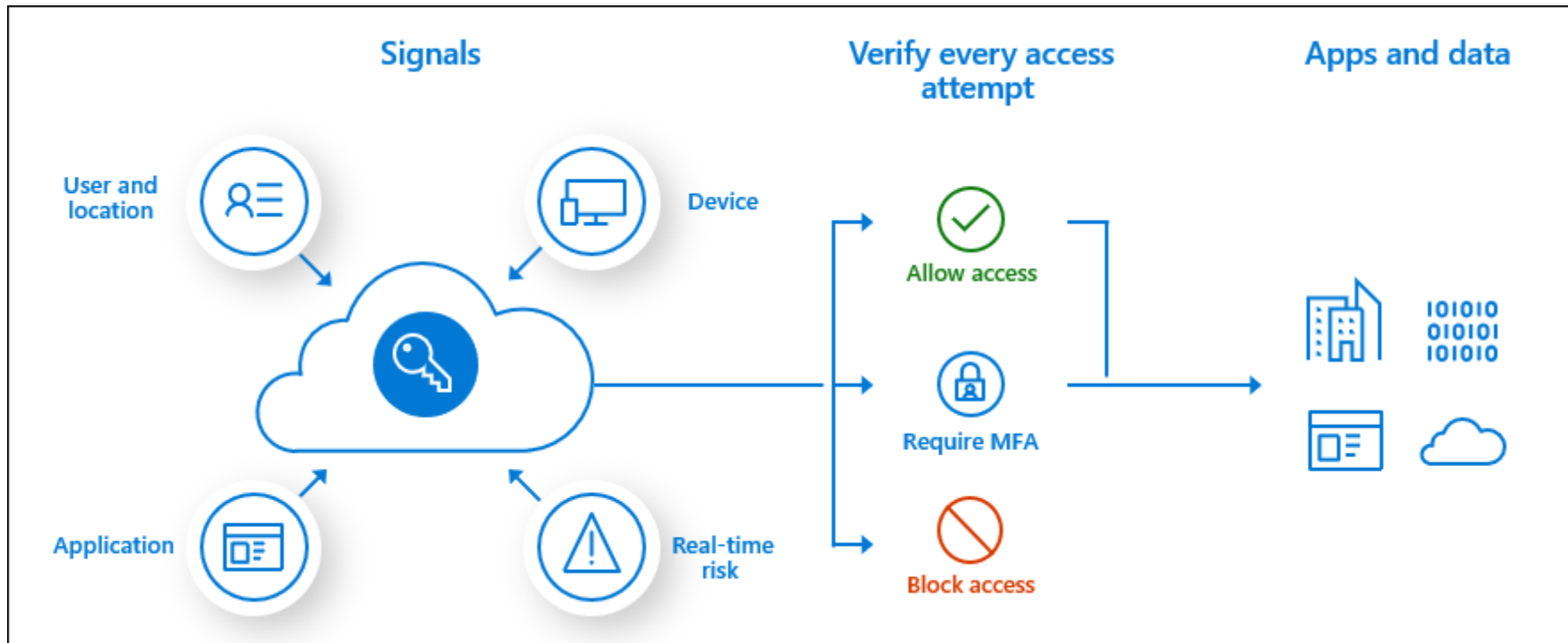
- Runs on premise
- Syncs custom AD attributes
- Supports pass-through authentication
- Object attribute filtering
- Password, device, and group writebacks

Connect Cloud Sync

- Runs in the cloud with a lightweight agent on premise
- Can sync multiple disconnected forests

<https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/what-is-cloud-sync>

Conditional Access Policies



[What is Conditional Access in Azure Active Directory? - Microsoft Entra | Microsoft Learn](#)

Microsoft Keynote at RSA 2022

>900 Password attacks per second
2X last year

1 hour 42 minutes Median time for an attacker to access your private data if you fall victim to a phishing email

1 hour 12 minutes Median time for an attacker to being moving laterally within your corporate network if a device is compromised

Microsoft at RSA 2020

> 1.2M Compromised accounts in January 2020

99.9% Compromised accounts did not have MFA

99% Password spray attacks used legacy authentication

> 97% Replay attacks used legacy authentication

Multi-Factor Authentication

- Three main supported methods
 - Voice phone call
 - SMS text code
 - App
- Microsoft Authenticator App is strongly recommended
 - Once setup it is the easiest to use
 - Simply approve on your mobile, no codes to enter
 - More secure
 - Still reports of SIM card swaps
 - Works over Wi-Fi as well as cellular data
 - More convenient when travelling
- Every account should require MFA, with a few exceptions
 - Emergency accounts
 - Guests (potentially, more to come)
- Eliminate “service” user accounts that have MFA disabled
 - Use Service Principals

Base Conditional Access Recommendations

- Create an emergency account
- Create separate cloud-only admin accounts
- Minimize the number of policies to reduce the risk of leaving gaps in your policies
- Block legacy authentication protocols
- Apply policies to all apps
- Define at least three sets of user groups
 - Admins
 - General users
 - External (guest) users
- Require MFA for all member users
- Define more restrictive policies for admins
- Block access from countries that you never expect a sign-in from

[Azure AD Conditional Access Policies Base Recommendations | Extranet User Manager](#)

Emergency Accounts

- Risk of mis-defining a policy and preventing admins getting access to fix the policy
 - Effectively blocks all access and locks you out of your tenant
- You can test your policies first in report-only mode
- Emergency accounts are a back-door way to get back
 - Excluded from all policies, and are a guaranteed way to get back in
 - Raises a security risk
- Require multiple people to gain access through the emergency account
 - Split the password into multiple components and having two or more admins have only their portion of the password in their private password vault
 - All admins must agree to use the emergency account
- Setup notifications to all administrators whenever the emergency account is used

MFA Scenarios

Admins

- Require MFA on every authentication

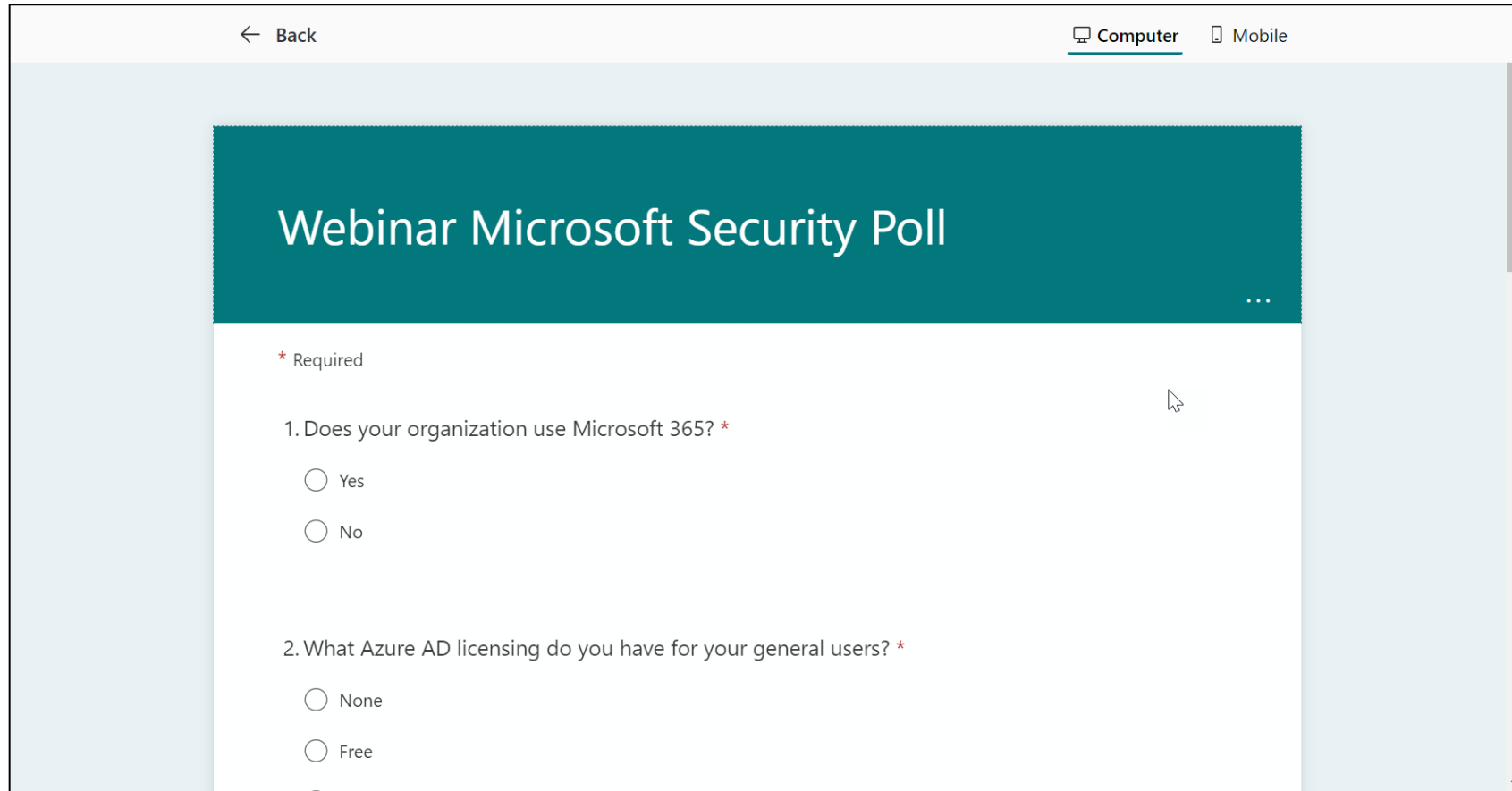
Members

- Rules can be more flexible
- Don't need MFA on every authentication
- Every x days on the same device
- Additional rules
 - Joined device
 - Geography
 - Identity Protection score
- Incorrect password

Guests

- Decide if MFA is required
- User experience and support cost to requiring it
- Doesn't need to be all or nothing
- Sensitivity labels are a good way to control this

Microsoft Forms Poll



The screenshot shows a Microsoft Forms poll interface. At the top, there is a navigation bar with a back arrow and the text 'Back'. To the right of the navigation bar, there are two tabs: 'Computer' (which is selected and underlined) and 'Mobile'. Below the navigation bar is a teal header with the title 'Webinar Microsoft Security Poll' and a three-dot menu icon on the right. The main content area contains two questions, both marked as required with a red asterisk. The first question is '1. Does your organization use Microsoft 365? *' with radio button options for 'Yes' and 'No'. The second question is '2. What Azure AD licensing do you have for your general users? *' with radio button options for 'None' and 'Free'. A mouse cursor is visible over the first question.

<https://forms.office.com/r/qzyCvW4ZF8>

Entra ID Portal Walkthrough

Microsoft Entra admin center


pcarson@envisionitdev...
ENVISION IT DEV (ENVISIONITDE...)

- Home
- Azure Active Directory
- Overview
- Users
- Groups
- Devices
- Applications
- Protect & secure
- Identity Governance
- External Identities
- Show more
- Permissions Management
- Verified ID
- Learn & support

Welcome to the Microsoft Entra admin center. We're building an integrated, easy-to-use approach to managing your entire identity infrastructure. We look forward to your feedback on our preview of the new admin center. Keep checking back for updates!
[Learn more](#)

Microsoft Entra


Secure access for a connected world



Azure Active Directory

Secure and manage identities to connect them with apps, devices and data.


[Go to Azure Active Directory](#)



Permissions Management

Discover, remediate, and monitor permission risks for any identity or resource.

[Go to Permissions Management](#)



Verified ID

Create, issue and verify decentralized identity credentials for secure interactions.

[Go to Verified ID](#)

[Give feedback](#)

<https://entra.microsoft.com>

Azure Portal B2B Links

[Cross Tenant Settings](#)

- B2B Collaboration
- B2B Direct Connect
- Trust Settings

[Identity Providers](#)

- Microsoft
- One-Time Passcode
- Google
- Facebook
- Custom SAML / WS-Federation

[External Collaboration Settings](#)

- Access, invite, and collaboration restrictions

Self-Service Sign Up

- [User Attributes](#)
- [API Connectors](#)
- [User Flows](#)

Lifecycle Management

- [Terms of Use](#)
- [Access Reviews](#)

[Company Branding](#)

Security

- [Conditional Access](#)
- [Terms of Use](#)

Monitoring

- [Sign-In Logs](#)
- [Audit Logs](#)
- [Diagnostic Logs](#)

envision IT ExtranetUserManager Microsoft Purview

Home

Compliance Manager

Data connectors

Reports

Policies

Solutions

Catalog

Communication compliance

Insider risk management

Privacy risk management

Subject rights requests

Settings

More resources

Customize navigation


Welcome to the Microsoft Purview compliance portal

[Intro](#) [Next steps](#) [Give feedback](#)

Welcome to the Microsoft Purview compliance portal, your home for managing compliance needs using integrated solutions to help protect sensitive info, manage data lifecycles, reduce insider risks, safeguard personal data, and more. [Learn more about the Microsoft Purview compliance portal](#)

[Next](#) Close

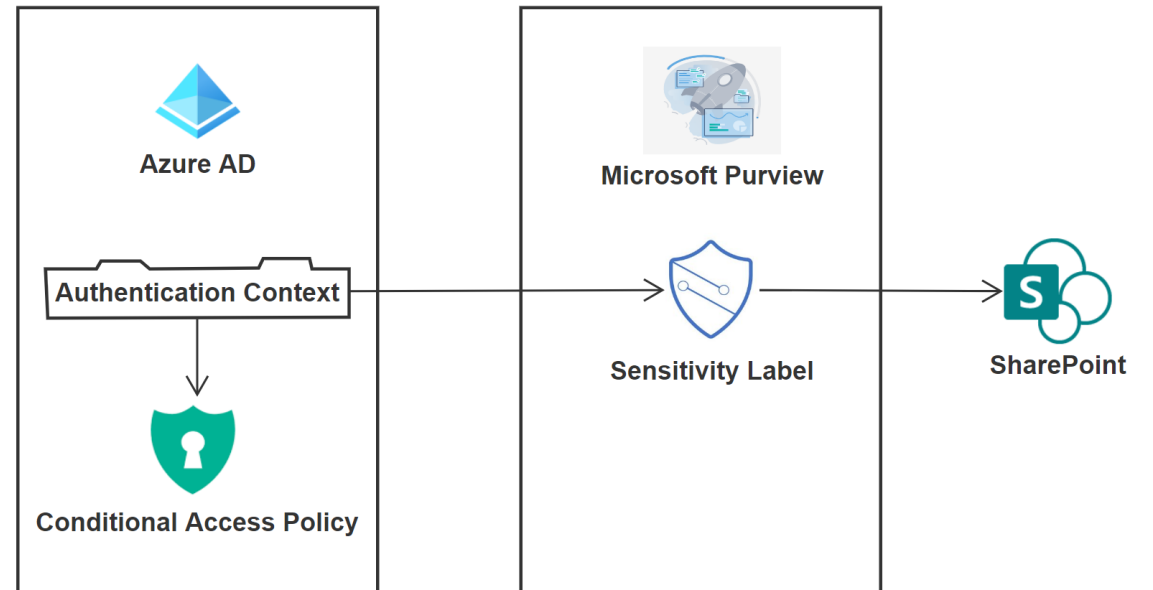
⚡ What's new? + Add cards



<https://compliance.microsoft.com>

Sensitivity Labels

- Labels can be applied to content in Microsoft 365
 - Emails
 - SharePoint sites and content
- Can be manually or automatically applied
- Can be leveraged in conditional access policies
- Can also enforce rights management and encryption
- Travels with the content regardless of location
- Can be applied to sharing rules



Authentication Context

Microsoft Azure Search resources, services, and docs (G+/)

Home > Envision IT Dev | Security > Security | Conditional Access > Conditional Access

Conditional Access | Authentication context (Preview)

Azure Active Directory

- Overview (Preview)
- Policies
- Insights and reporting
- Diagnose and solve problems

Manage

- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Authentication context (Preview)**
- Classic policies

Monitoring

- Sign-in logs
- Audit logs

Troubleshooting + Support

+ New authentication context Refresh Got feedback?

Get started

Authentication context (Preview)

Authentication context is used to secure application data and actions in apps like SharePoint and Microsoft Cloud App Security. The list of recommended configurations below provide an overview of all the actions that are required. After configuring them, apply authentication contexts to cloud apps, SharePoint sites and other resources. [Learn more](#)

Configuration steps

Step	Documentation
Configure authentication contexts	Learn more
Assign Conditional Access policies to the authentication context	Learn more
Tag resources with an authentication context	Learn more

[Cloud apps, actions, and authentication context in Conditional Access policy - Azure Active Directory - Microsoft Entra | Microsoft Learn](#)

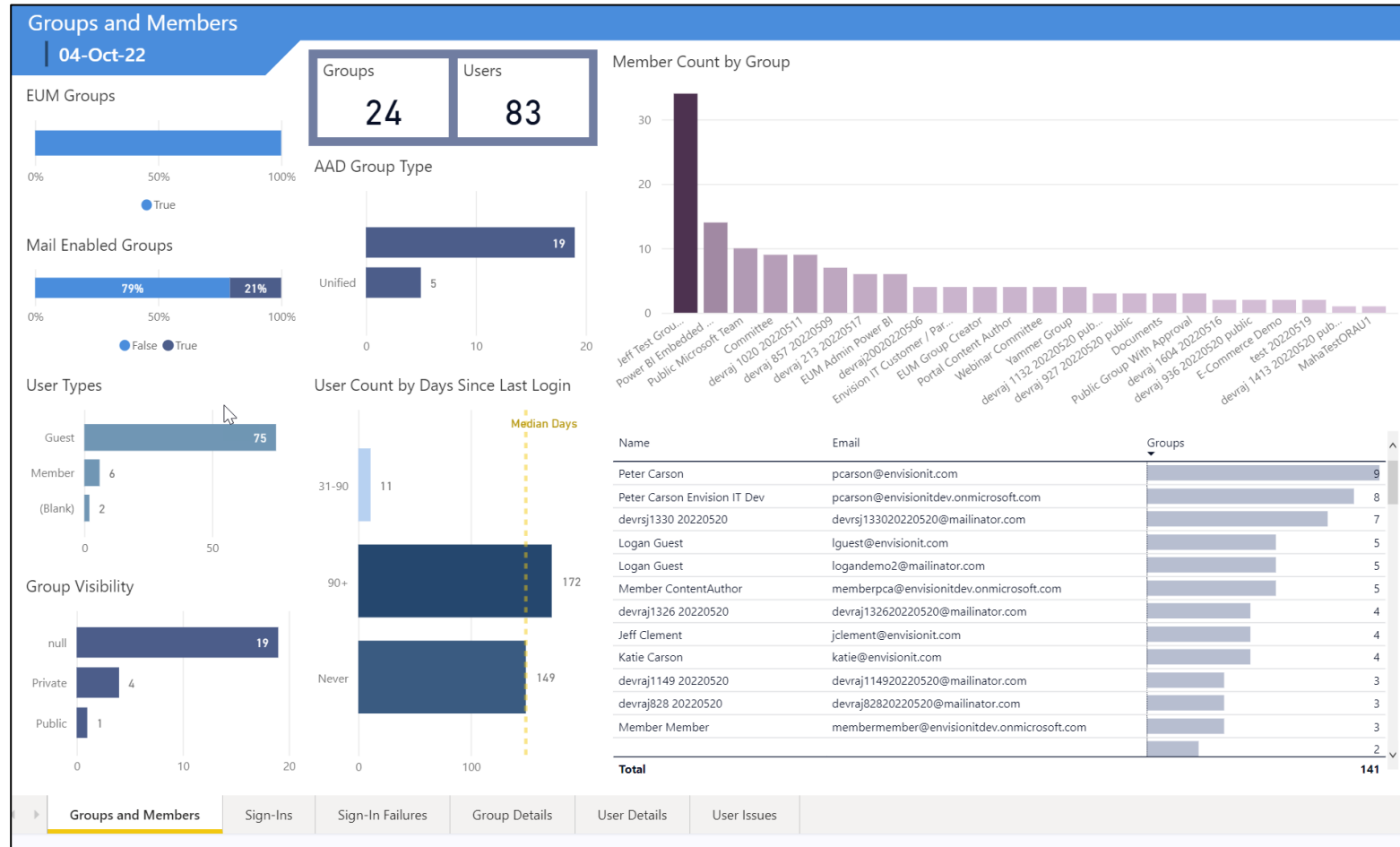
Azure AD B2B Resources

The screenshot shows the 'ExtranetUserManager' website. The navigation bar includes 'Platform', 'Resources', 'Pricing', 'About', and 'Support'. The main content area features a breadcrumb 'Home > Resources' and a large heading 'Azure AD B2B Collaboration Resources'. Below this is a section titled 'About Azure' with a paragraph of text. A 'Featured Article' section highlights 'Power BI Azure AD Users and Groups Dashboard' with a date of 'Jun 23, 2022' and a 'Download Technical Guide' button. A 'Related Assets' section shows 'Configuring Azure AD B2B for External Users'. On the right side, there are two call-to-action buttons: 'Learn more AZURE AD B2B RESOURCES' and 'Stay in the loop NEWSLETTER SIGN UP'. A 'Support' button is located at the bottom right of the page.

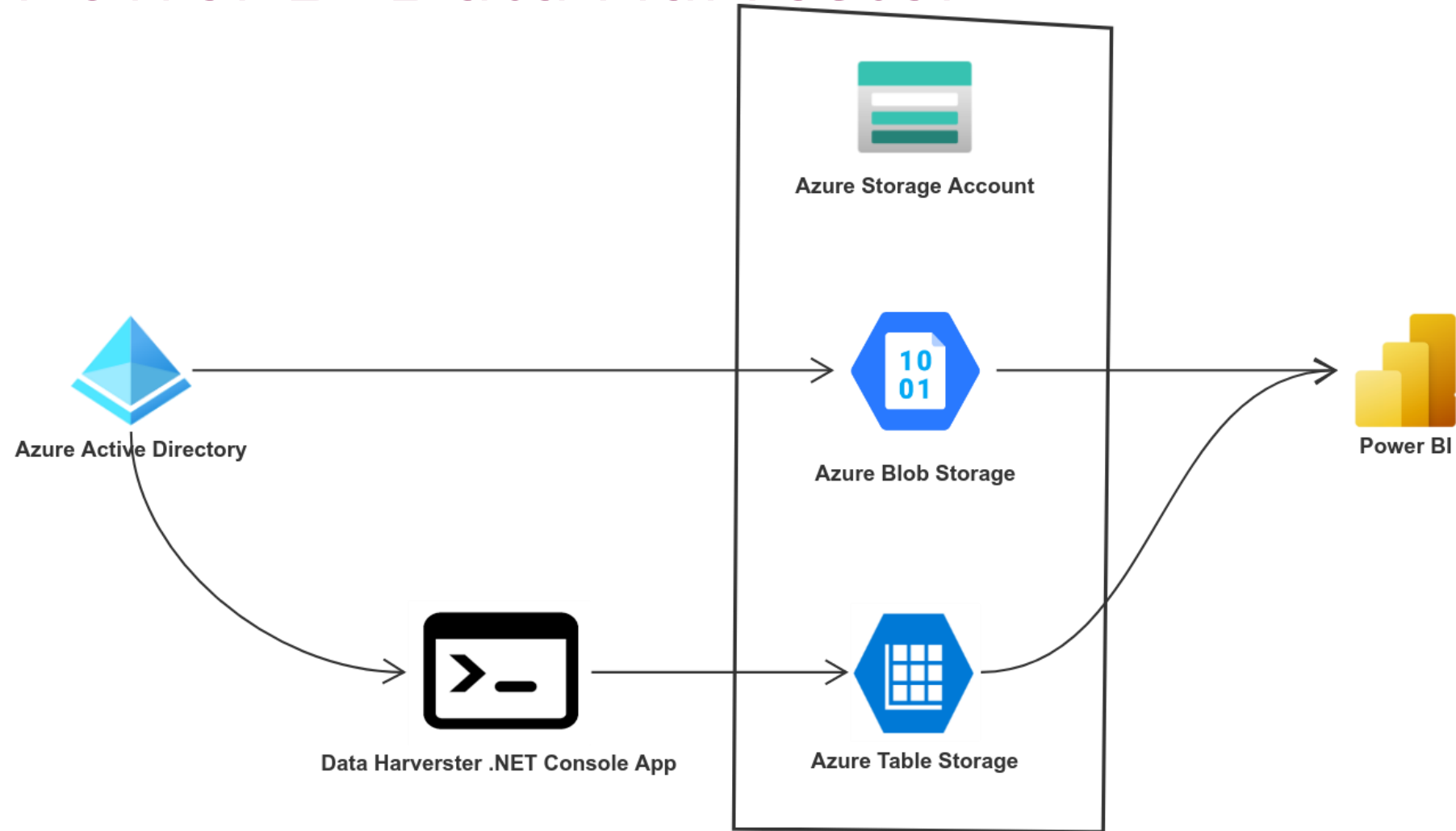
<https://www.extranetusermanager.com/resources/Azure-AD-B2B-Collaboration-Resources>

https://github.com/extranet-user-manager/EUM_AzureADPowerBI

Azure AD Power BI Dashboard


Groups and Members
Sign-Ins
Sign-In Failures
Group Details
User Details
User Issues

Power BI Data Harvester



Azure AD B2B Health

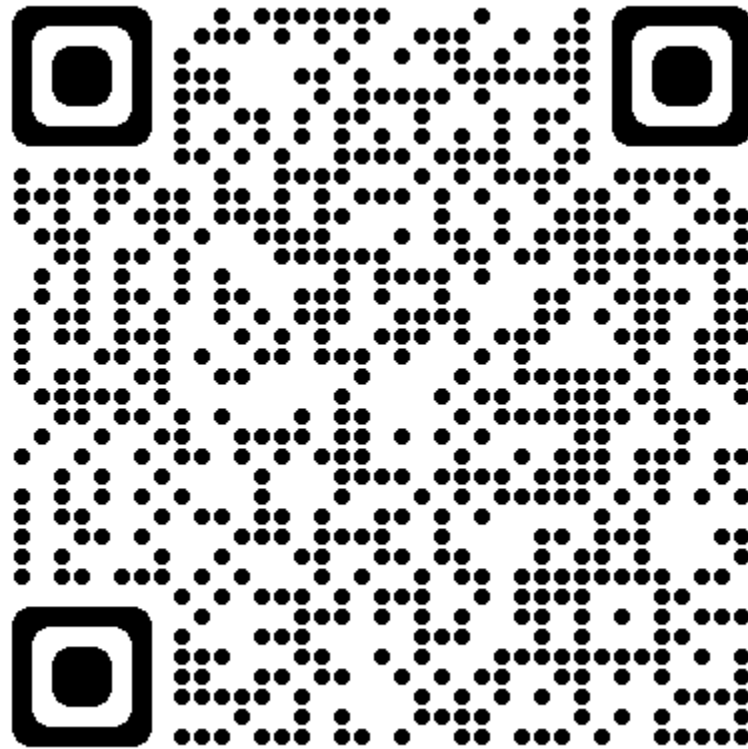
- User Type Not Populated
 - Users created before Aug 2014 when B2B first launched
- Mismatch Between Email and UPN
 - Can cause confusion when signing in
- Missing Email
 - Email is required for direct sign in without accepting the Microsoft invitation
- Broken External Tenants
 - Misconfigured or abandoned Azure AD tenants
- Unaccepted Invitations
 - Invitations are no longer needed
 - Users that were invited when it was required and didn't accept can't sign in
 - Resending the invitation still requires them to use the invitation
 - Deleting and re-inviting them allows them to sign in without the invitation
- Conflicting Microsoft Account
 - Brings up work/school or personal account dialog
 - Doesn't always prompt
 - Causes confusion

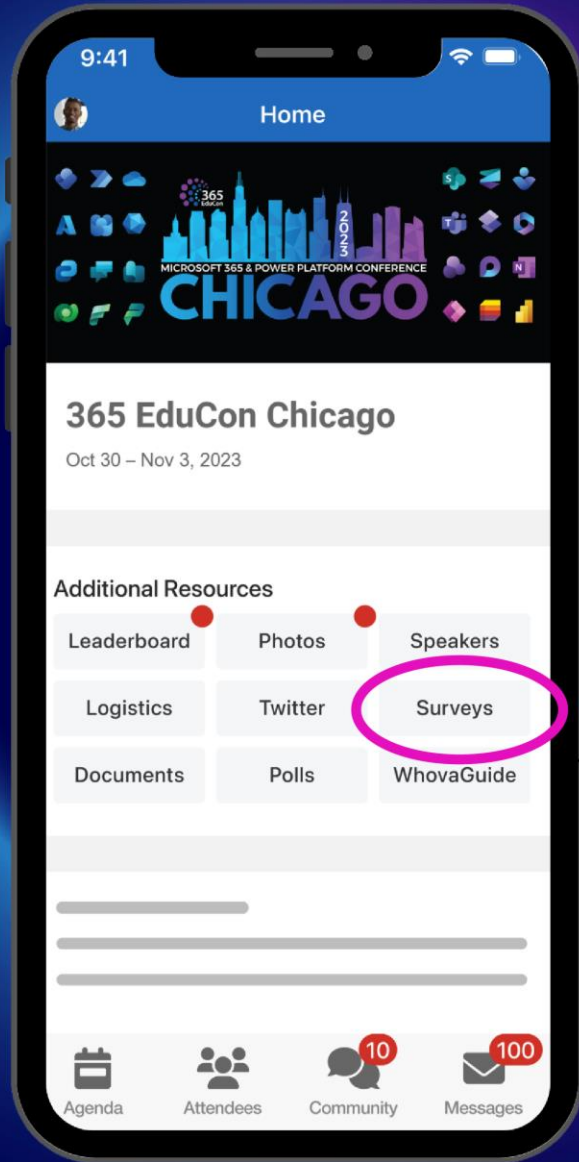
Thank you!

Questions?



Presentation Download





How was the session?

Search for *Whova* in the App Store or Google Play



Fill out the Session Surveys in the **365 EduCon Chicago Event** and be eligible to win **PRIZES!**