

The logo for SECTOR 2021 Hybrid Event features the word "SECTOR" in a bold, white, sans-serif font. A stylized white outline of the CN Tower is positioned behind the letter "C". The background of the logo is a dark blue gradient with a starry, particle-like effect. Below the main text, the words "2021 HYBRID EVENT" are written in a smaller, white, sans-serif font.

SECTOR

2021 HYBRID EVENT

Azure AD and Microsoft 365 Security Fundamentals

Wed, Oct 5, 2022

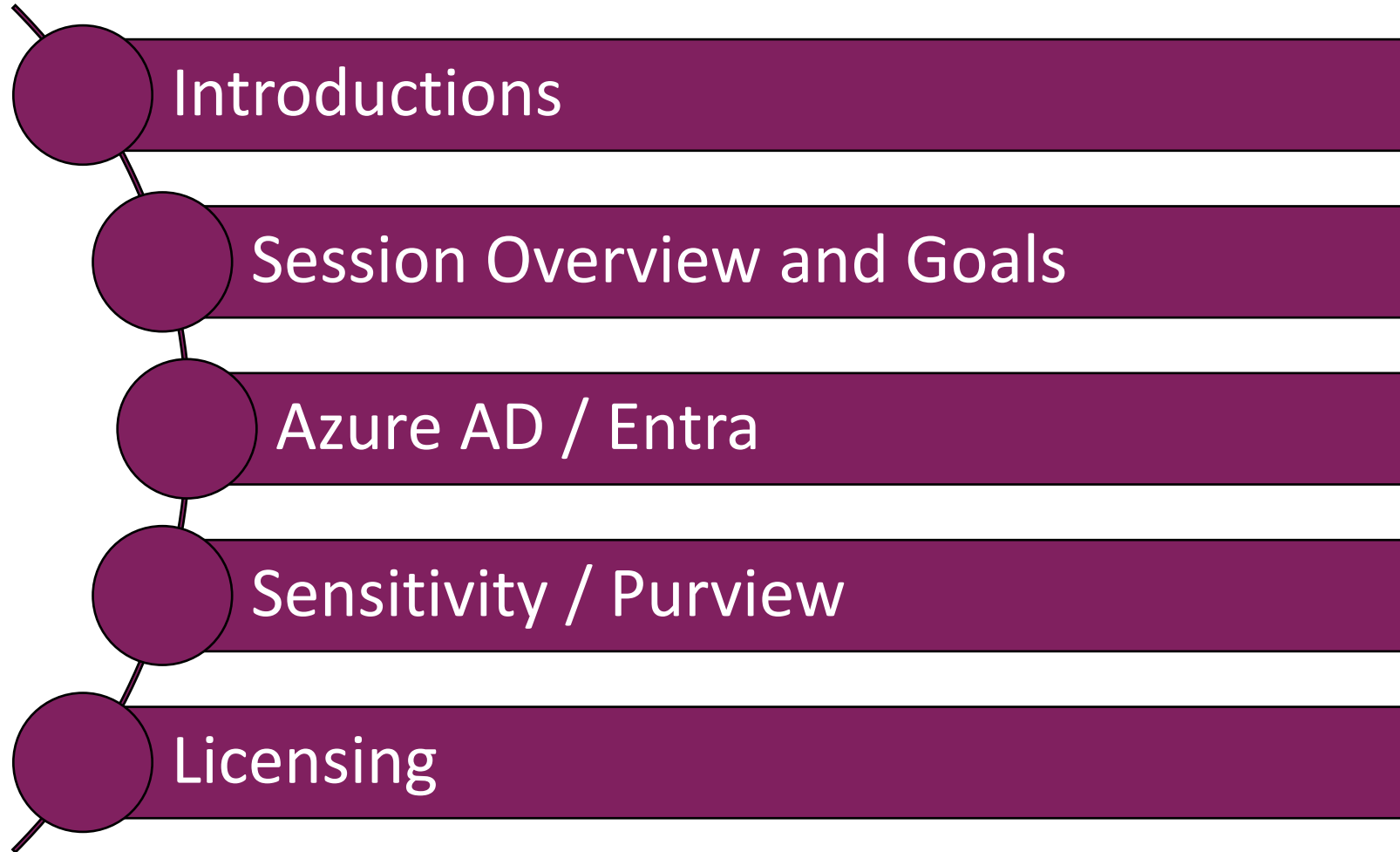
Peter Carson



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



Agenda



Session Overview and Goals

Azure Active Directory 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



Azure Active Directory

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](https://www.microsoft.com/en-us/security/business/microsoft-entra)

Azure AD Versions

- **Free**
 - Included with any commercial online service
- **Office 365**
 - Office 365 E1, E3, E5, F1 and F3 subscriptions
- **Security Defaults available in Free and Office 365**
 - Mobile App MFA for all users - no configuration
 - Blocks legacy authentication protocols
- **Azure AD P1**
- **Azure AD P2**

[Azure AD Multi-Factor Authentication versions and consumption plans - Microsoft Entra | Microsoft Learn](#)

Azure AD P1 vs. P2

Azure AD Premium P1

- **Conditional Access**
 - Multi-factor authentication
 - **Terms of Use**
- Hybrid Identities
- Password protection (custom banned passwords)
- Advanced Security and Usage Reports
- **Conditional Access based on group, location, and device status**
- **Azure Information Protection integration**
- And [Much More](#)

\$7.70 / user / month

Azure AD Premium P2

- Everything offered in P1
- Identity Protection
- **Privileged Identity Management**
- Access reviews
- Entitlement Management (Preview)

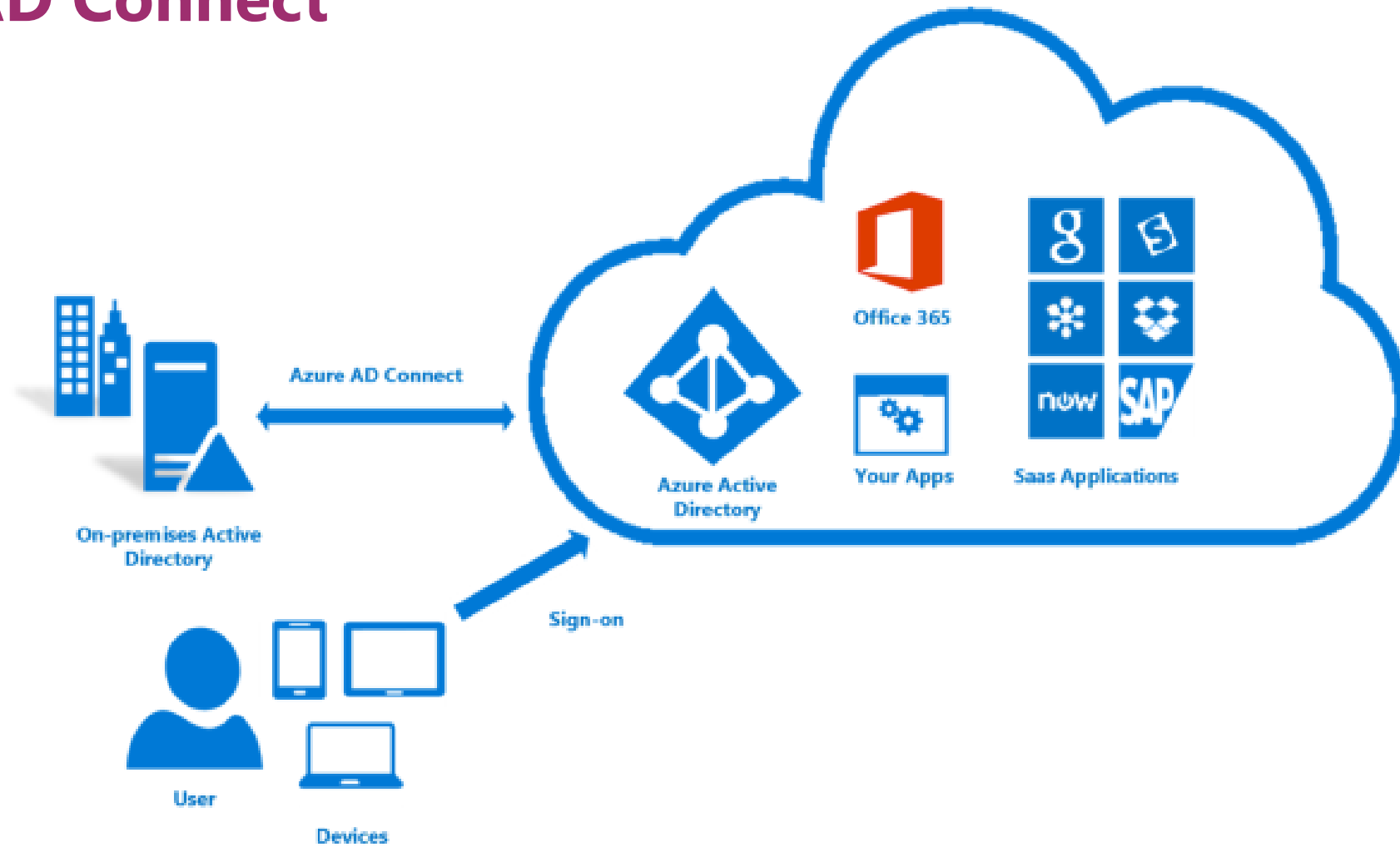
\$11.50 / user / month

Types of Azure AD Users and Authentication

Member - Synced	Member – Cloud Only	Guest
<ul style="list-style-type: none">• Synced from on premise Active Directory• Authentication options<ul style="list-style-type: none">• Password hash synchronization (PHS)• Pass-through authentication (PTA)• Federation	<ul style="list-style-type: none">• Account only exists in the cloud• Authentication options<ul style="list-style-type: none">• Cloud password• Federation	<ul style="list-style-type: none">• Invited in<ul style="list-style-type: none">• Microsoft 365• Azure guest invitation• Authentication Options<ul style="list-style-type: none">• 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

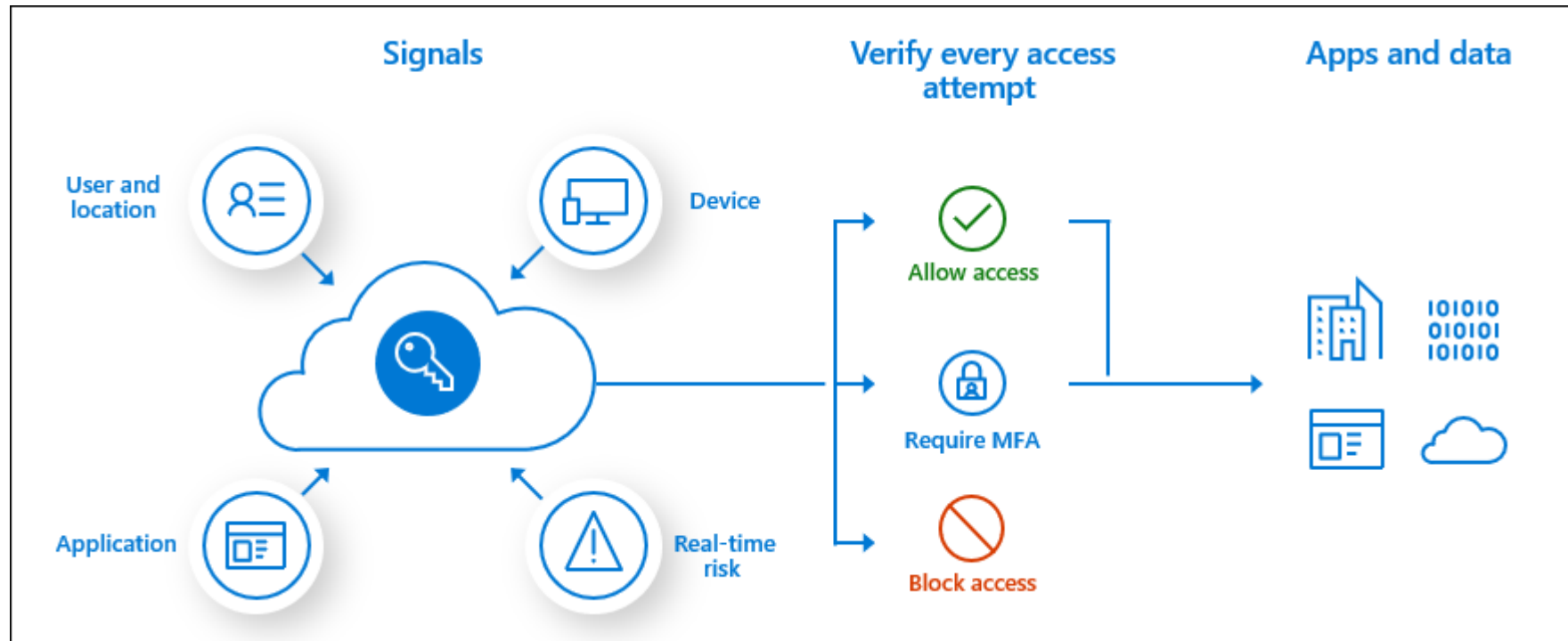
- **Runs on premise**
- **Syncs custom AD attributes**
- **Supports pass-through authentication**
- **Object attribute filtering**
- **Password, device, and group writebacks**

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**

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**

Azure AD Portal Walkthrough

Microsoft Entra admin center

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

- 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](#)

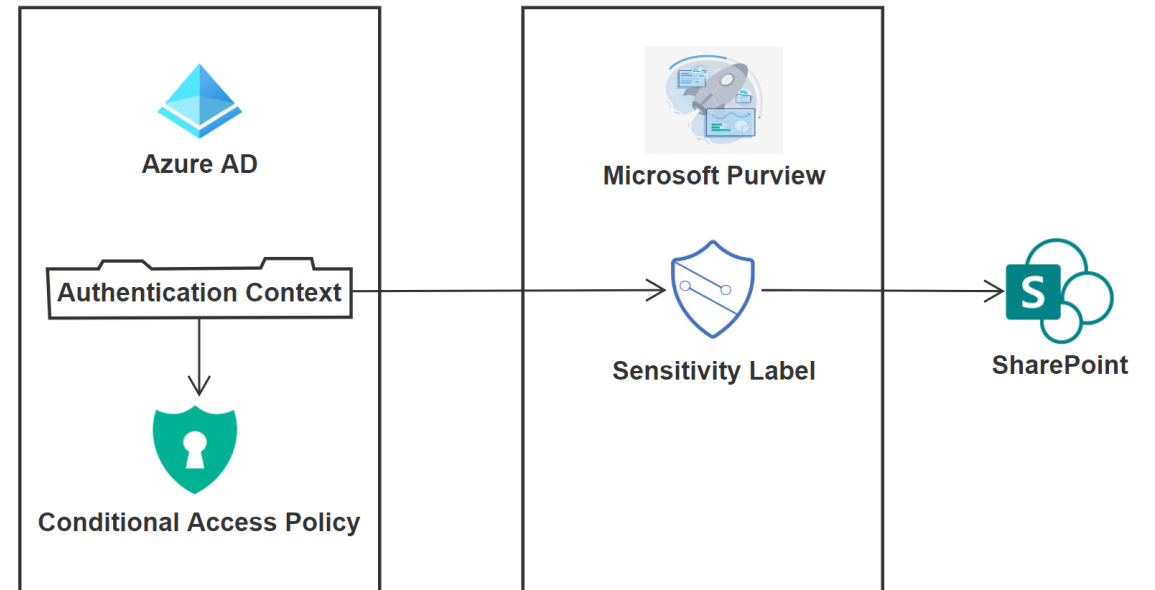
[Next](#) Close

[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**



Sensitivity Labels Walkthrough

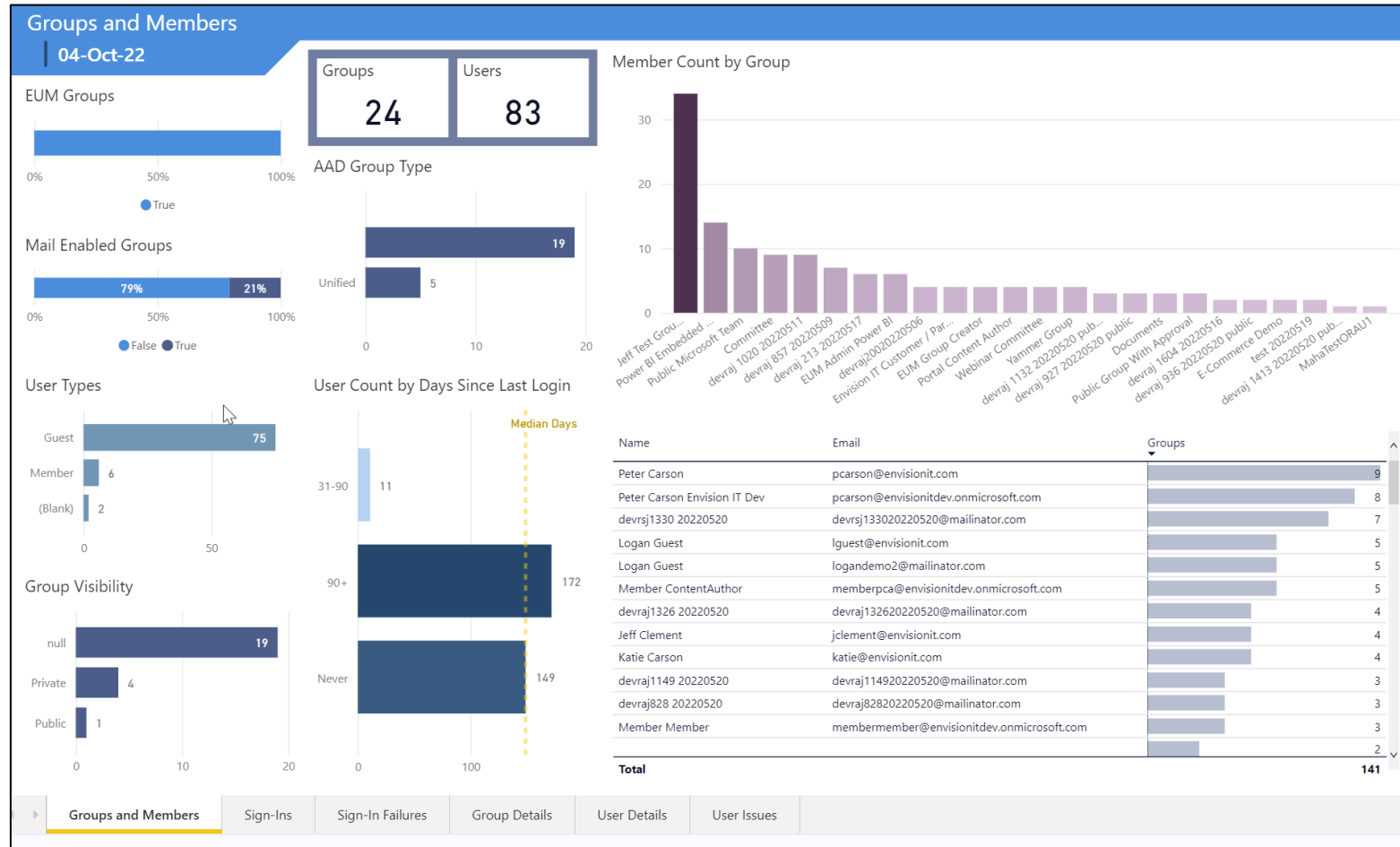
Azure AD B2B Resources

The screenshot shows the 'ExtranetUserManager' website with a navigation bar containing '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 explaining the site's purpose. A 'Featured Article' section highlights 'Power BI Azure AD Users and Groups Dashboard I' with a date of 'Jun 23, 2022' and a 'Download Technical Guide' button. A 'Related Assets' section includes 'Configuring Azure AD B2B for External Users' and a 'Support' button. A right-hand sidebar contains 'Learn more' and 'AZURE AD B2B RESOURCES' buttons, and 'Stay in the loop' and 'NEWSLETTER SIGN UP' buttons.

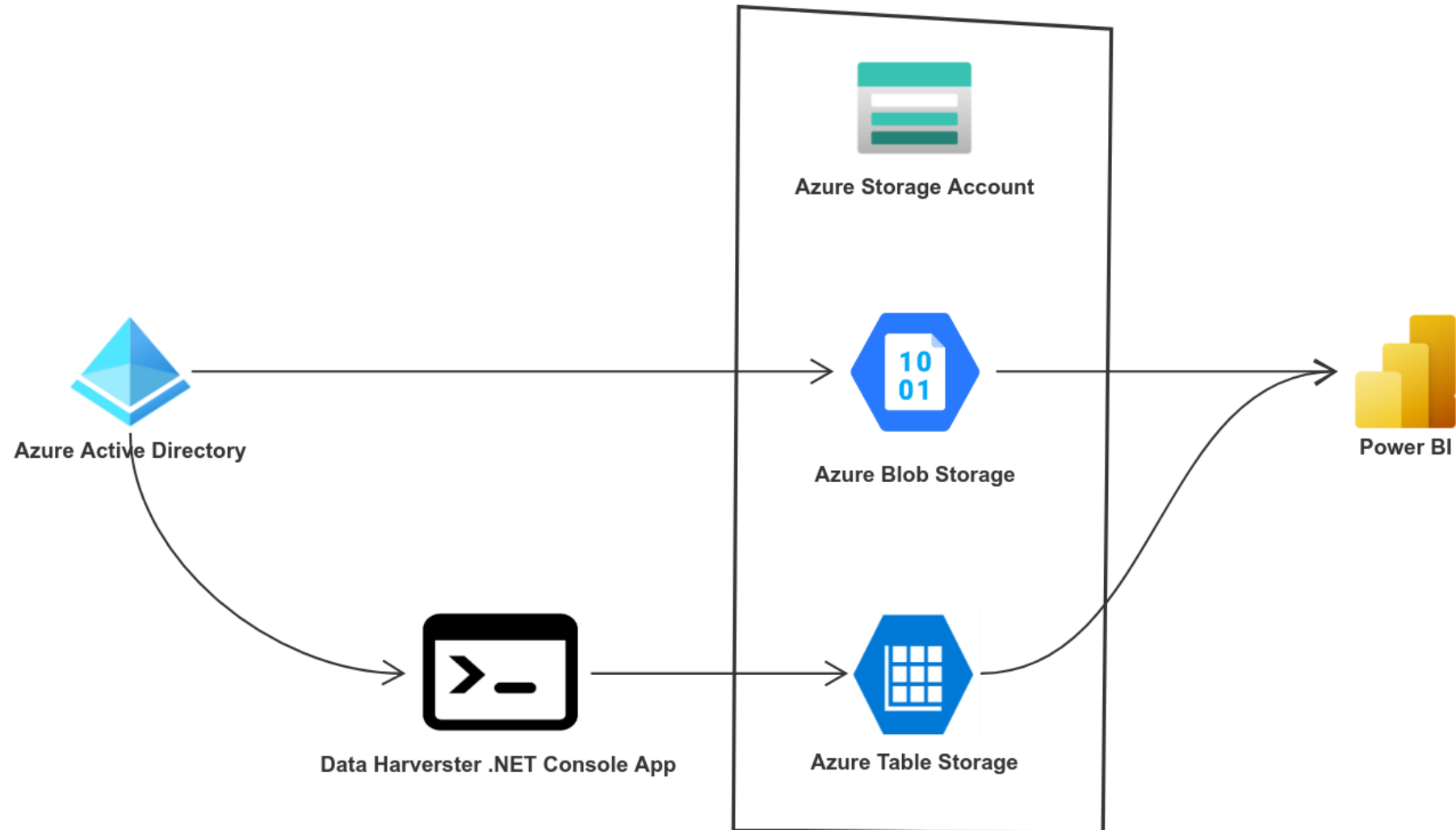
<https://www.extranetusermanager.com/resources/Azure-AD-B2B-Collaboration-Resources>

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

Azure AD Power BI Dashboard



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
- **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



External Users in Teams

External Users in Teams

B2B Guests

- **User exists in the external Team's Azure AD**
- **All the B2B controls apply**
- **Guests need to switch their Teams to the external tenant**
 - Lose their home tenant's Teams, notifications, feeds
- **Can use different browser profiles for different tenants**

Teams Connect

- **Needs to be enabled on both tenants**
 - More for organization to organization sharing
- **No tenant switching**
- **Shared channels appear with all the home Teams and channels**
- **Also appear in home activity feed**

Shared Channels vs. Private Channels

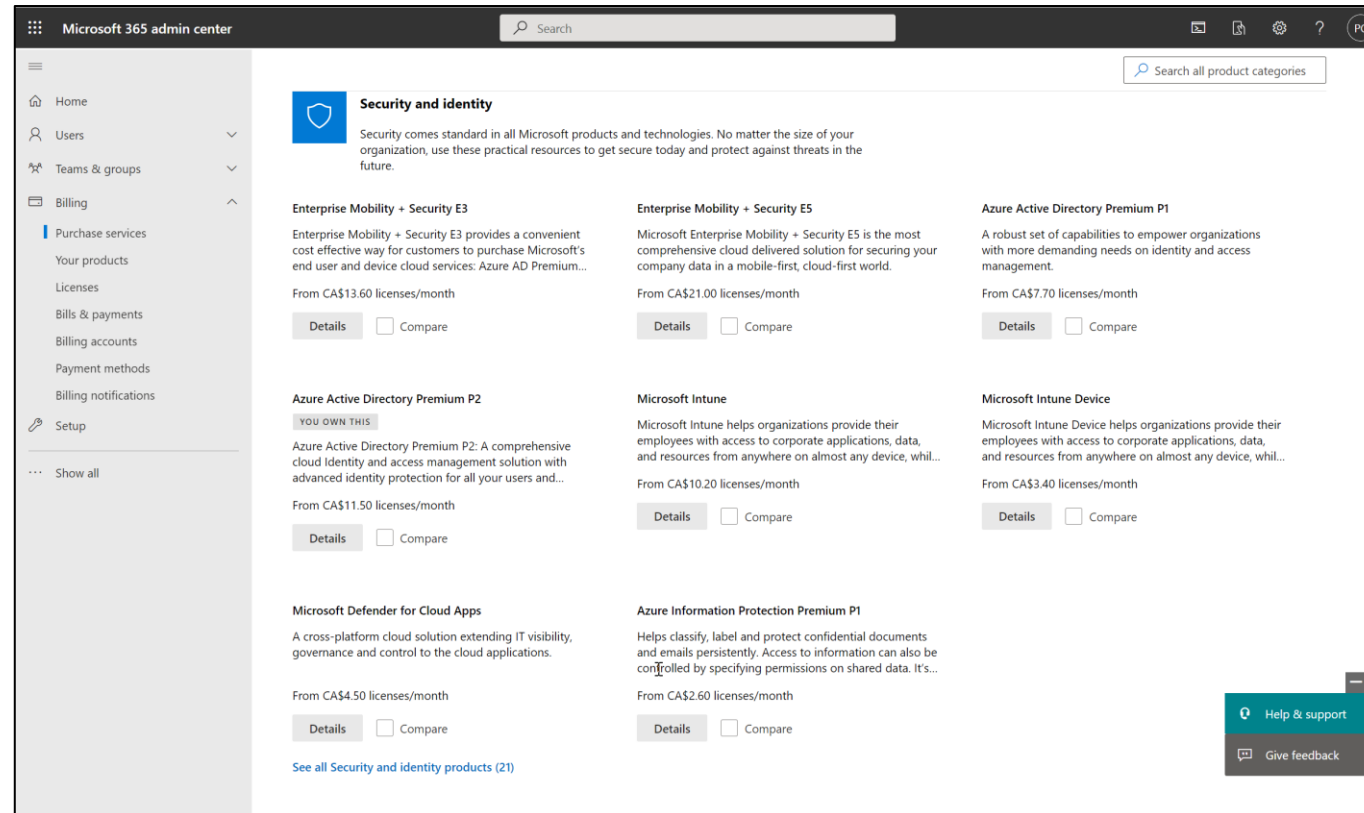
- **Both channel styles create a channel site collection for documents**
- **Both have Teams restrictions on Apps and features**
- **Private channels let you invite a subset of the parent Team's members**
- **Shared channels let you invite anyone allowed in the tenant**

- **Department team that is private to that department**
 - All company channel for two way communication with the organization
- **Outbound connections don't need to be setup**
 - Just add members of the tenant
- **This is also a good Yammer use case**

[How We Use Teams Shared Channels | Extranet User Manager](#)

Licensing

Microsoft 365 Admin Center



<https://admin.microsoft.com>

Sensitivity Labelling

For manual sensitivity labeling, the following licenses provide user rights:

- Microsoft 365 E5/A5/G5/E3/A3/G3/F1/F3/Business Premium (Information Protection for Office 365 – Standard should be enabled if E5 license only has been assigned)
- Enterprise Mobility + Security E3/E5
- Office 365 E5/A5/E3/A3
- AIP Plan 1
- AIP Plan 2

For both client and service-side automatic sensitivity labeling, the following licenses provide user rights:

- Microsoft 365 E5/A5/G5
- E5 Compliance
- Microsoft 365 E5/A5/G5 Information Protection and Governance
- Office 365 E5/A5/G5

For client-side automatic sensitivity labeling only, the following license provides user rights:

- Enterprise Mobility + Security E5/A5/G5
- AIP Plan 2

To apply and view sensitivity labels in Power BI and to protect data when it's exported from Power BI to Excel, PowerPoint, or PDF, the following licenses provide user rights:

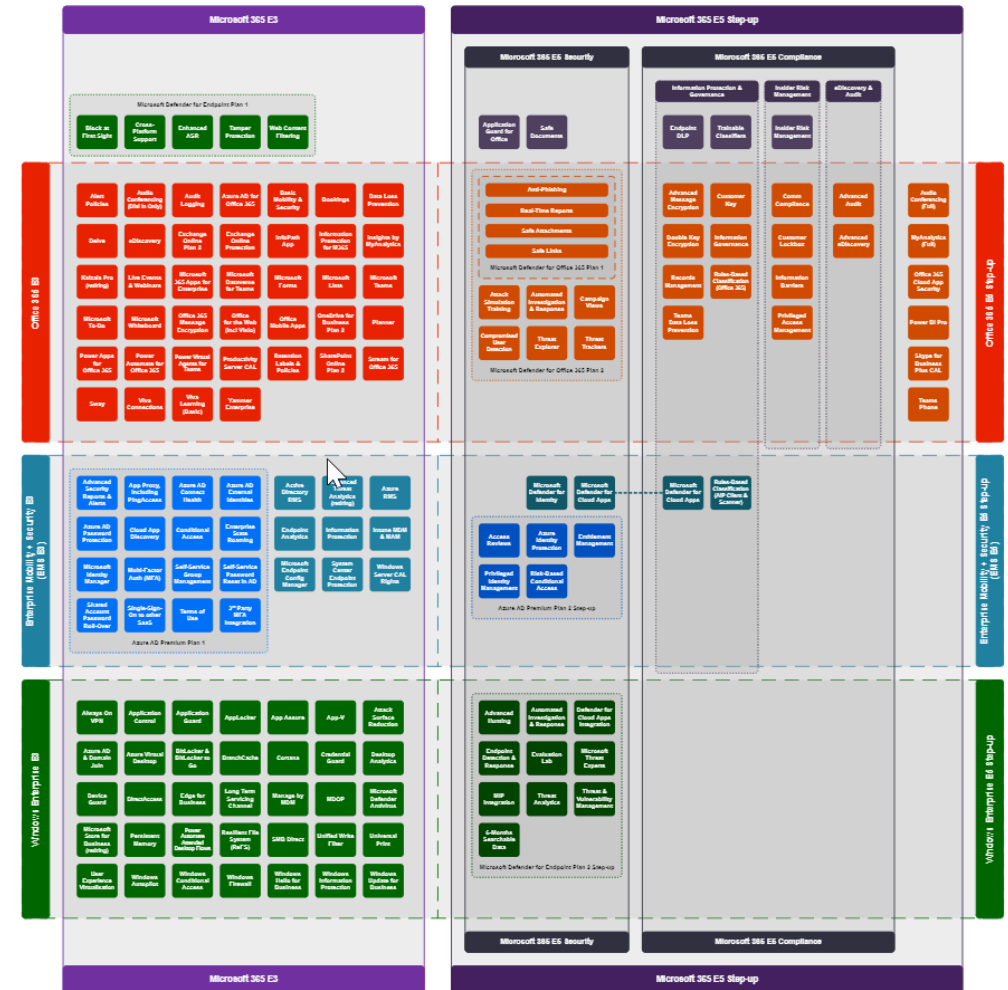
- Microsoft 365 E5/A5/G5/E3/A3/G3/F1/F3/Business Premium
- Enterprise Mobility + Security E3/E5
- AIP Plan 1
- AIP Plan 2

[Microsoft 365 guidance for security & compliance - Service Descriptions | Microsoft Learn](#)

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
- **First 50,000 MAUs are free for both Premium P1 and Premium P2 features**

	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 \(microsoft.com\)](https://www.microsoft.com/licensing/terms)
- Internal employee users are not eligible
 - Consider [Microsoft 365 F1](#)

Thank you!

Questions?

