Azure AD and Microsoft 365 Security Fundamentals

https://www.extranetusermanager.com/resources/events/webinar-2022-11-15-azure-ad-and-microsoft-365-security-fundamentals

www.eum.co

Tue, Nov 15, 2022

Logan Guest

- Sales and Marketing Manager, Extranet User Manager
- lguest@envisionit.com
- www.extranetusermanager.com

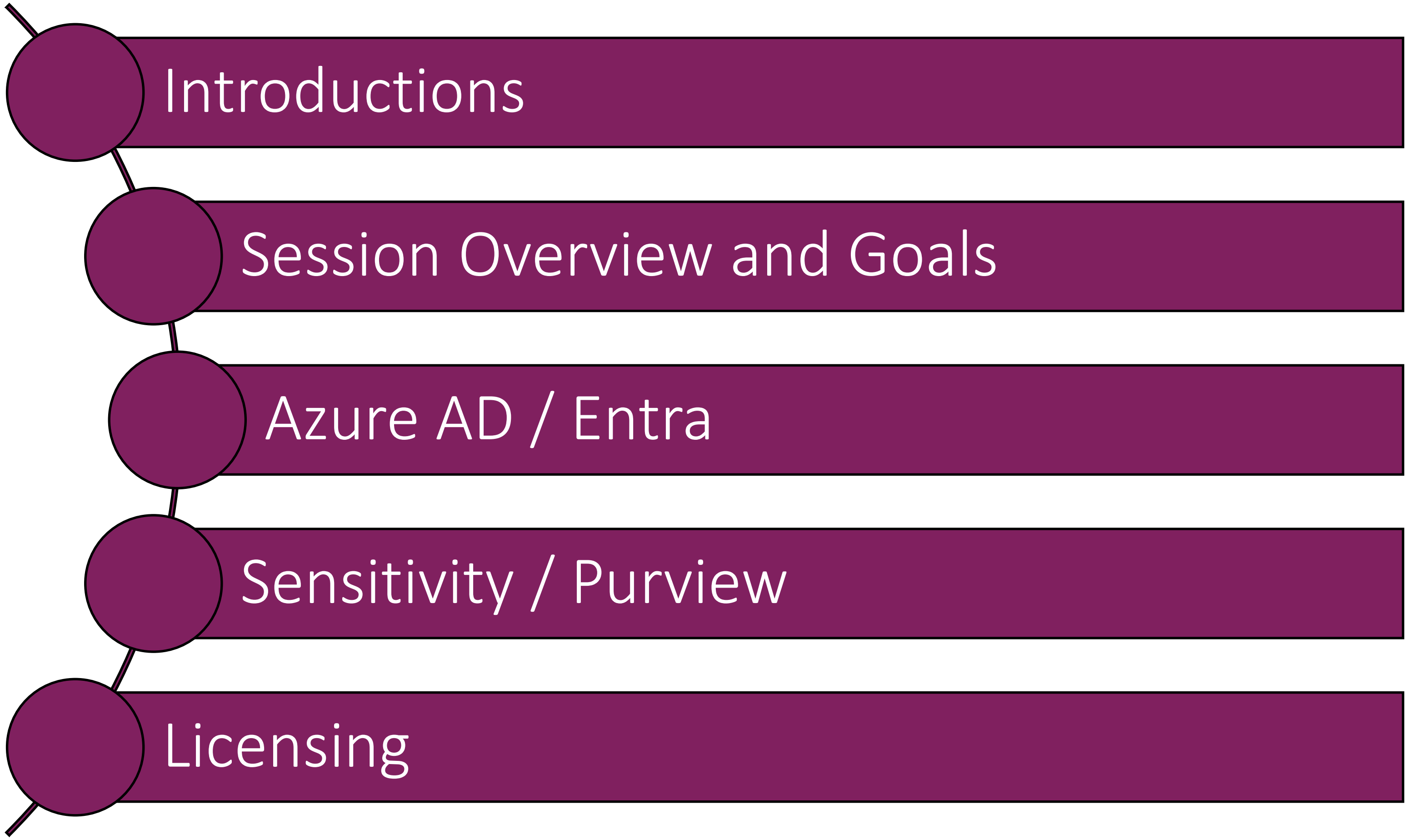
Teams Meeting Etiquette

- This is a regular Teams meeting.
- Chat is open throughout the webinar.
- Feel free to ask questions or make comments through chat at any time.
- Please stay on mute. If you'd like to join the conversation, please ask on chat and wait for an invitation.
- Welcome, enjoy, and learn!

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



- Introductions
- Session Overview and Goals
- Azure AD / Entra
- Sensitivity / Purview
- Licensing

Session Overview and Goals

Azure Active Directory is the core security infrastructure

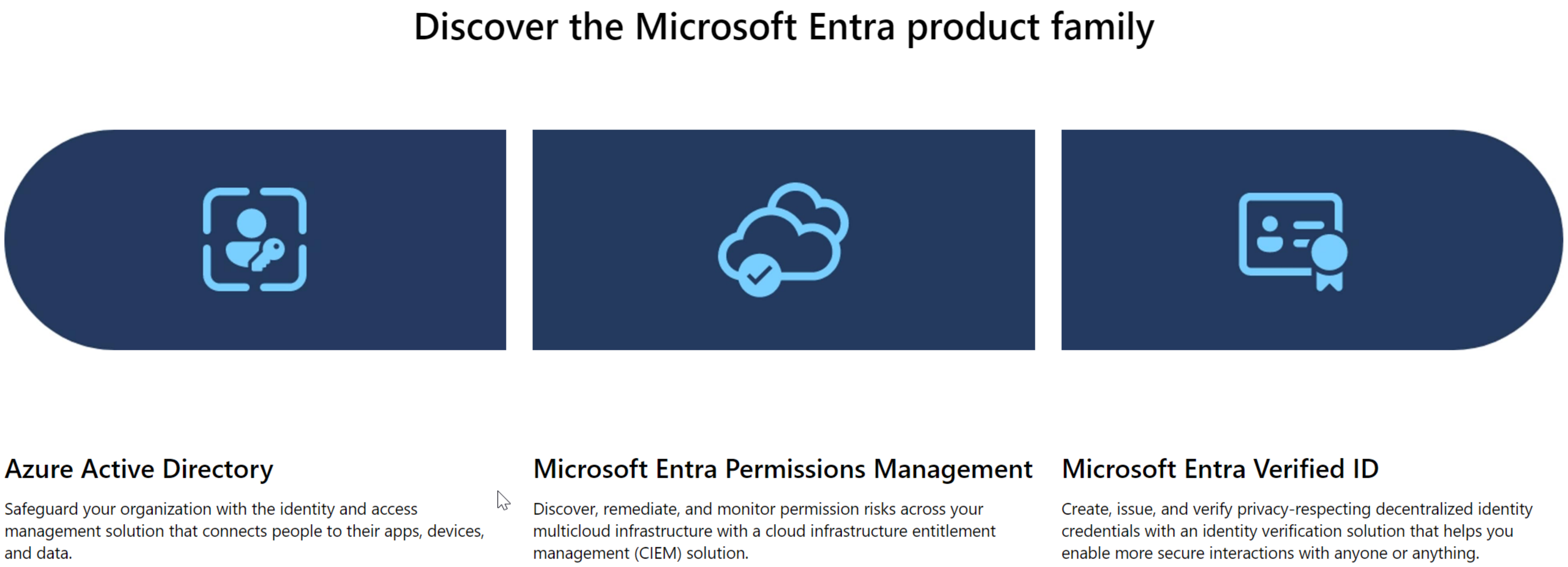
Features depend on licenses

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]

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

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

Member – Cloud Only

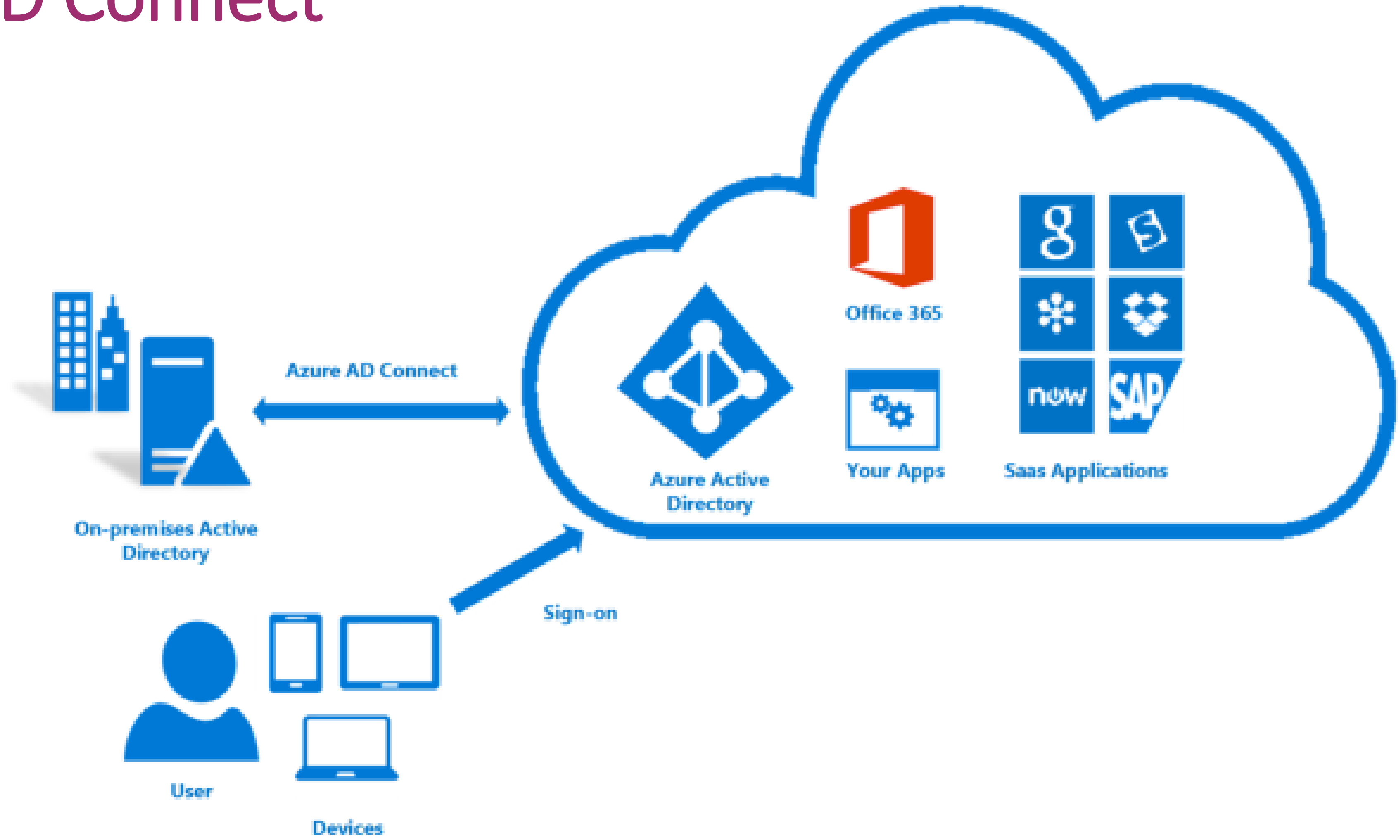
- Account only exists in the cloud
- Authentication options
  - Cloud password
  - Federation

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

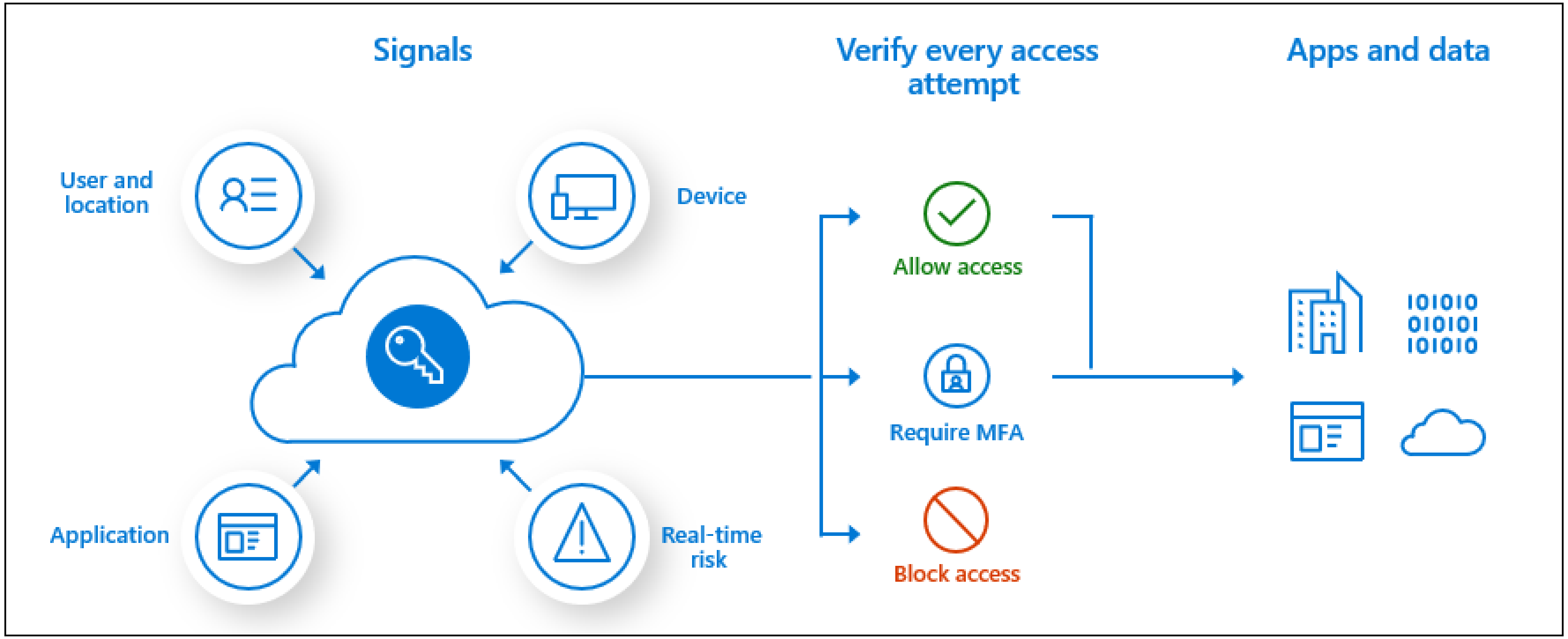
- Runs on premise
- Syncs custom AD attributes
- Supports pass-through authentication
- Object attribute filtering
- Password, device, and group writebacks

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

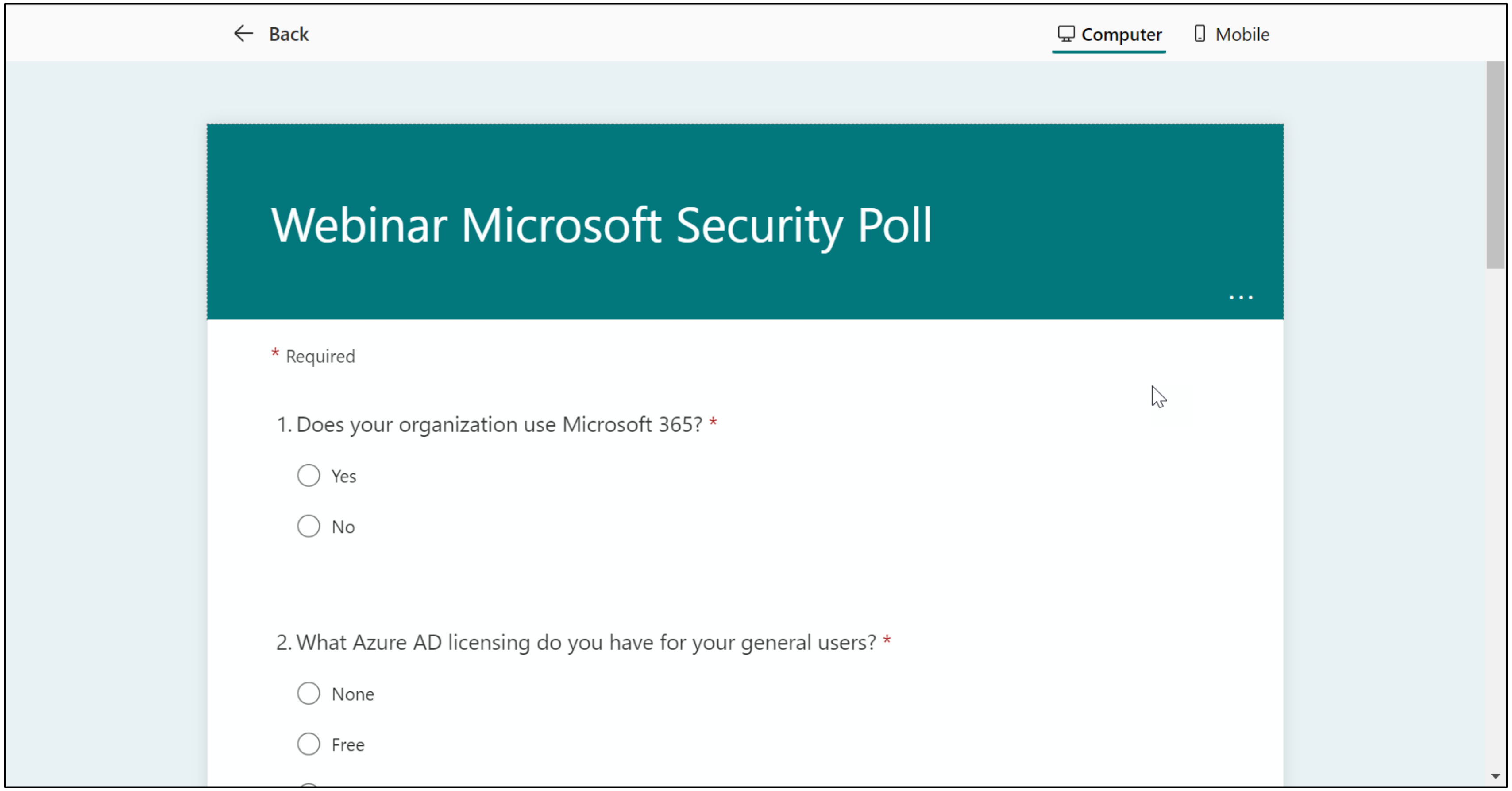
Members

- 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



Webinar Microsoft Security Poll

* Required

1. Does your organization use Microsoft 365? *

○ Yes

○ No

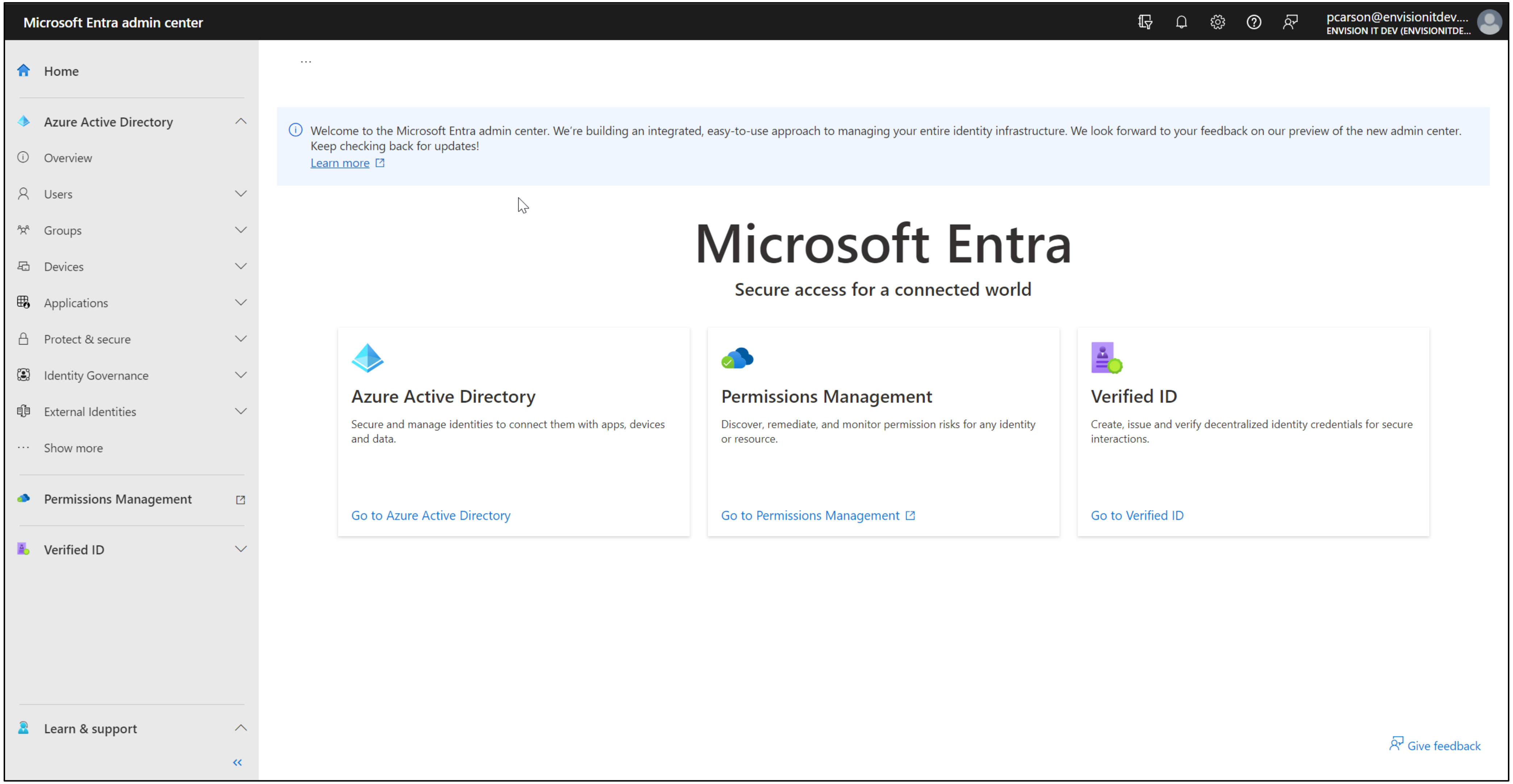
2. What Azure AD licensing do you have for your general users? *

○ None

○ Free

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

Azure AD Portal Walkthrough



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

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

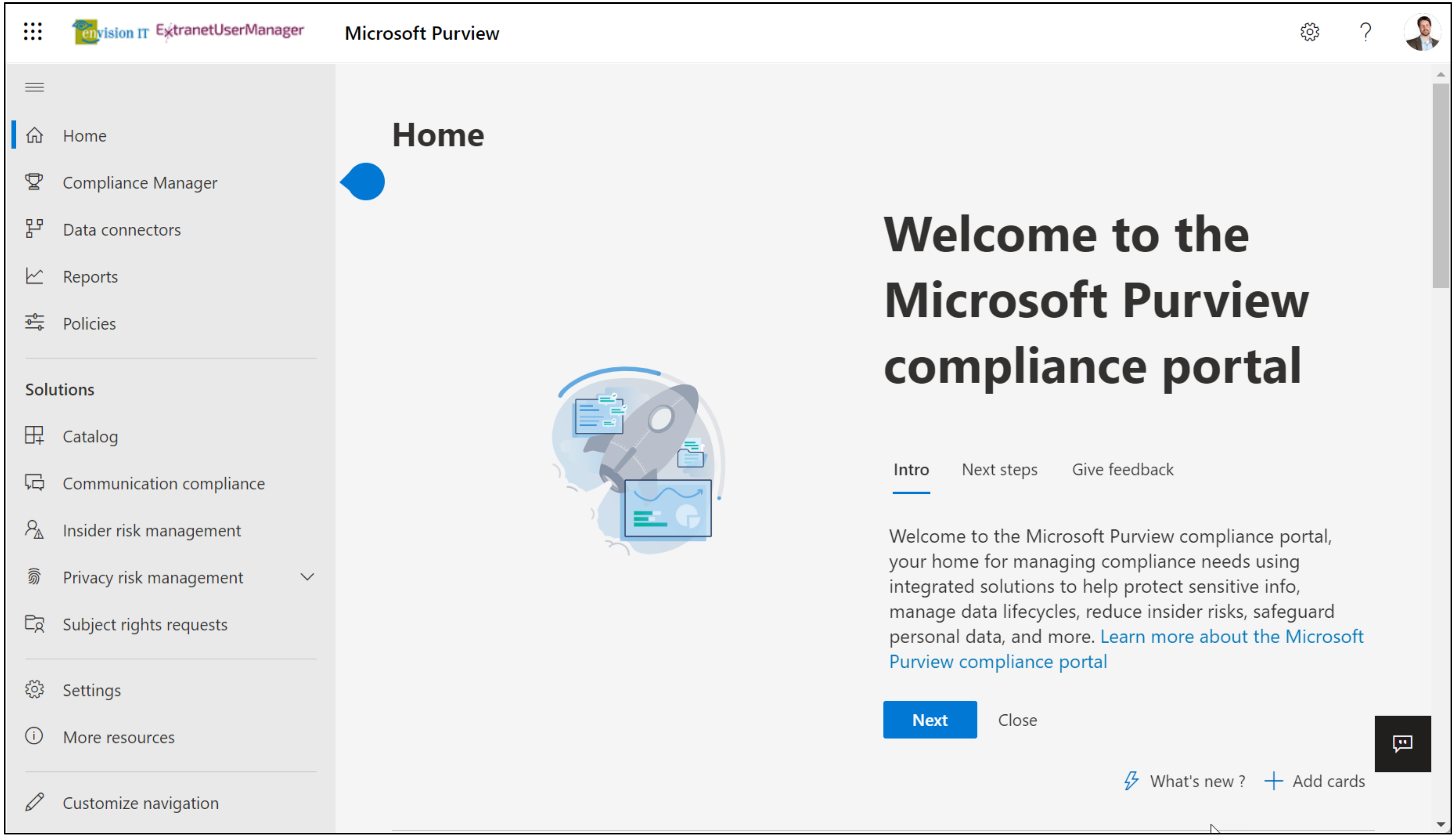
Company Branding

Security

- Conditional Access
- Terms of Use

Monitoring

- Sign-In Logs
- Audit Logs
- Diagnostic Logs



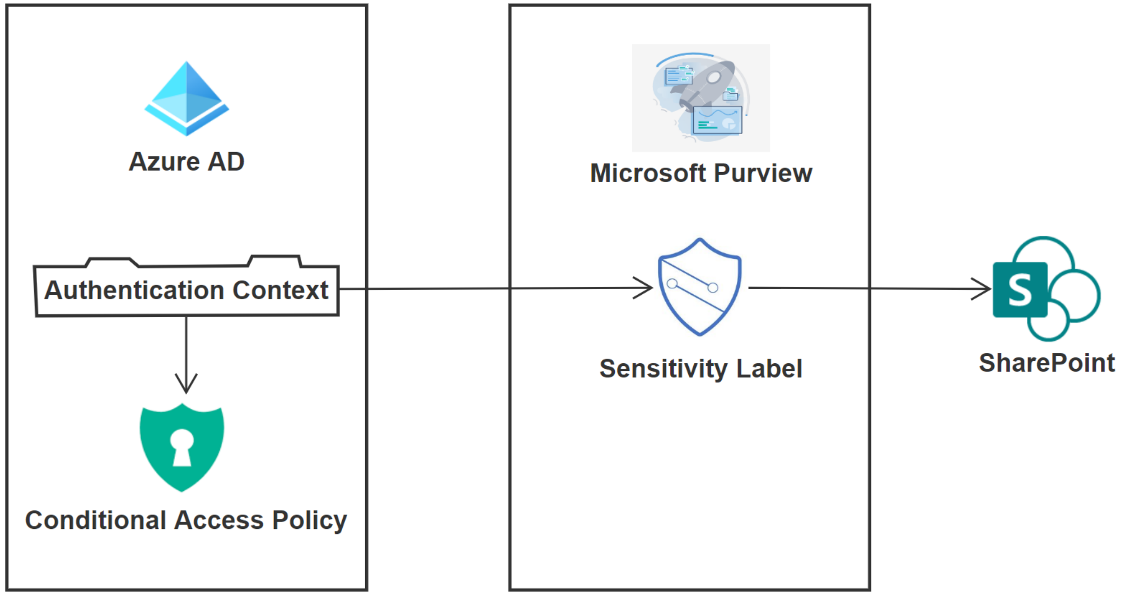
Welcome to the Microsoft Purview compliance portal

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

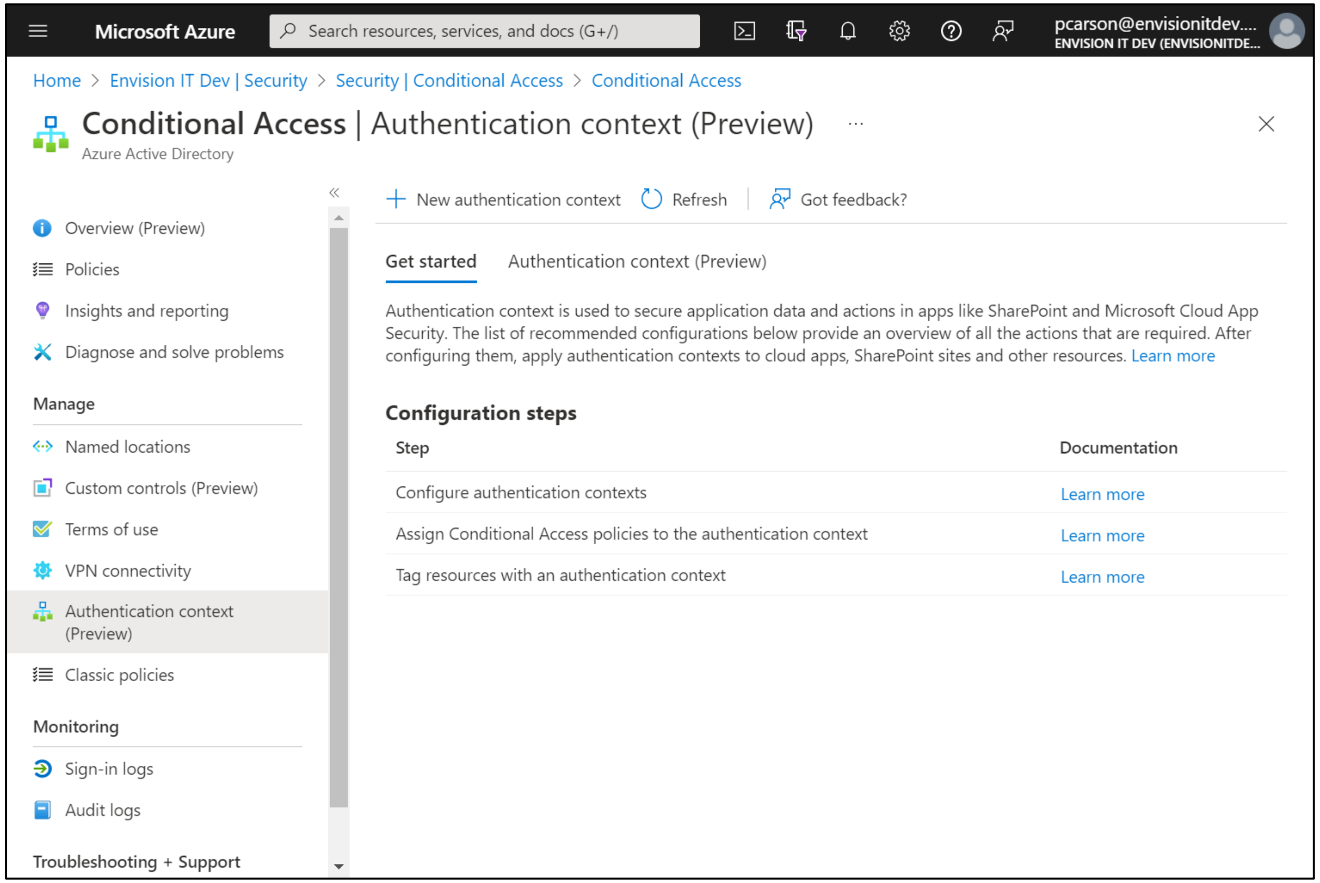
https://compliance.microsoft.com

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

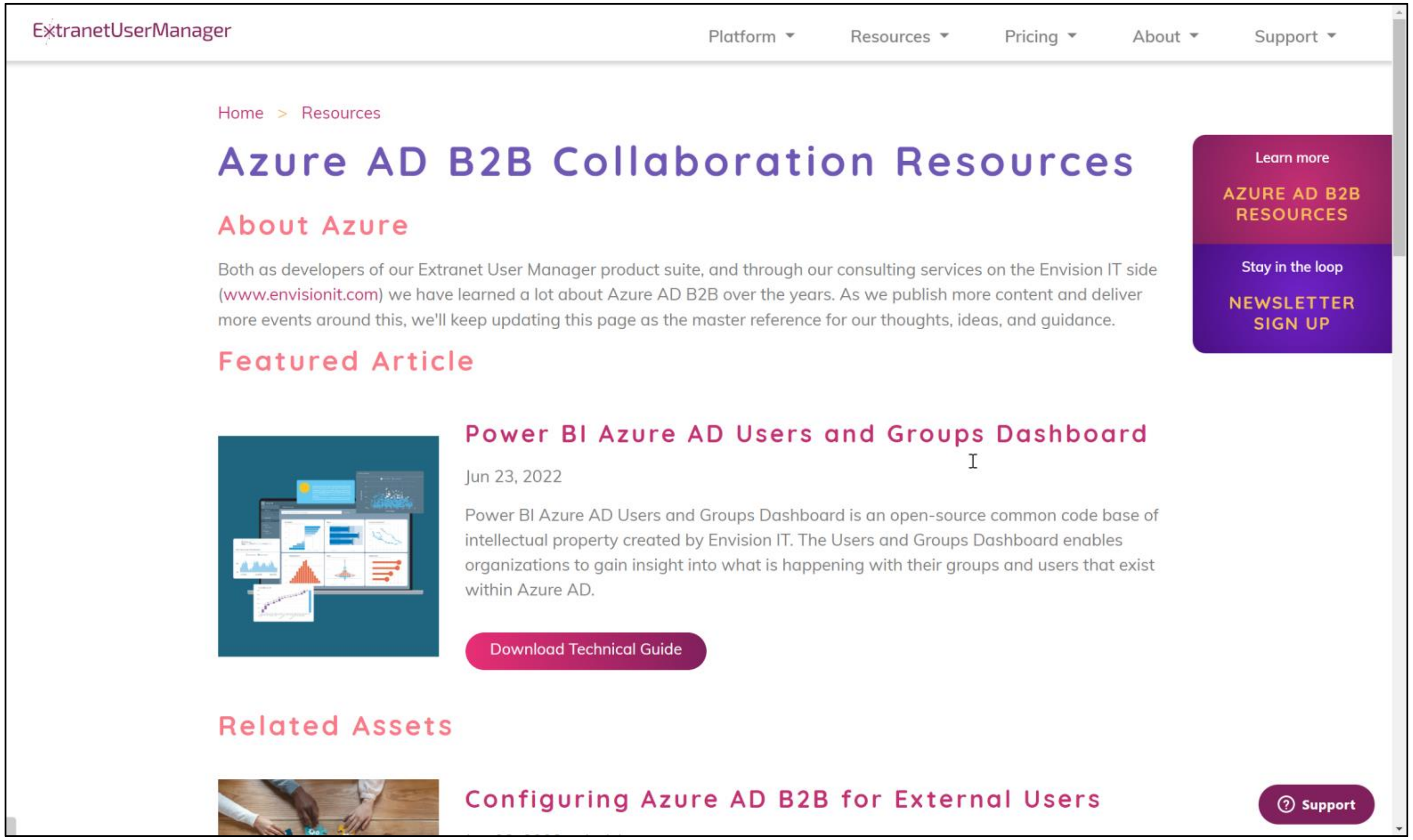
Configuration steps

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]

Sensitivity Labels Walkthrough

Azure AD B2B Resources



Home > Resources

Azure AD B2B Collaboration Resources

About Azure

Both as developers of our Extranet User Manager product suite, and through our consulting services on the Envision IT side (www.envisionit.com) we have learned a lot about Azure AD B2B over the years. As we publish more content and deliver more events around this, we'll keep updating this page as the master reference for our thoughts, ideas, and guidance.

Featured Article

Power BI Azure AD Users and Groups Dashboard

Jun 23, 2022

Power BI Azure AD Users and Groups Dashboard is an open-source common code base of intellectual property created by Envision IT. The Users and Groups Dashboard enables organizations to gain insight into what is happening with their groups and users that exist within Azure AD.

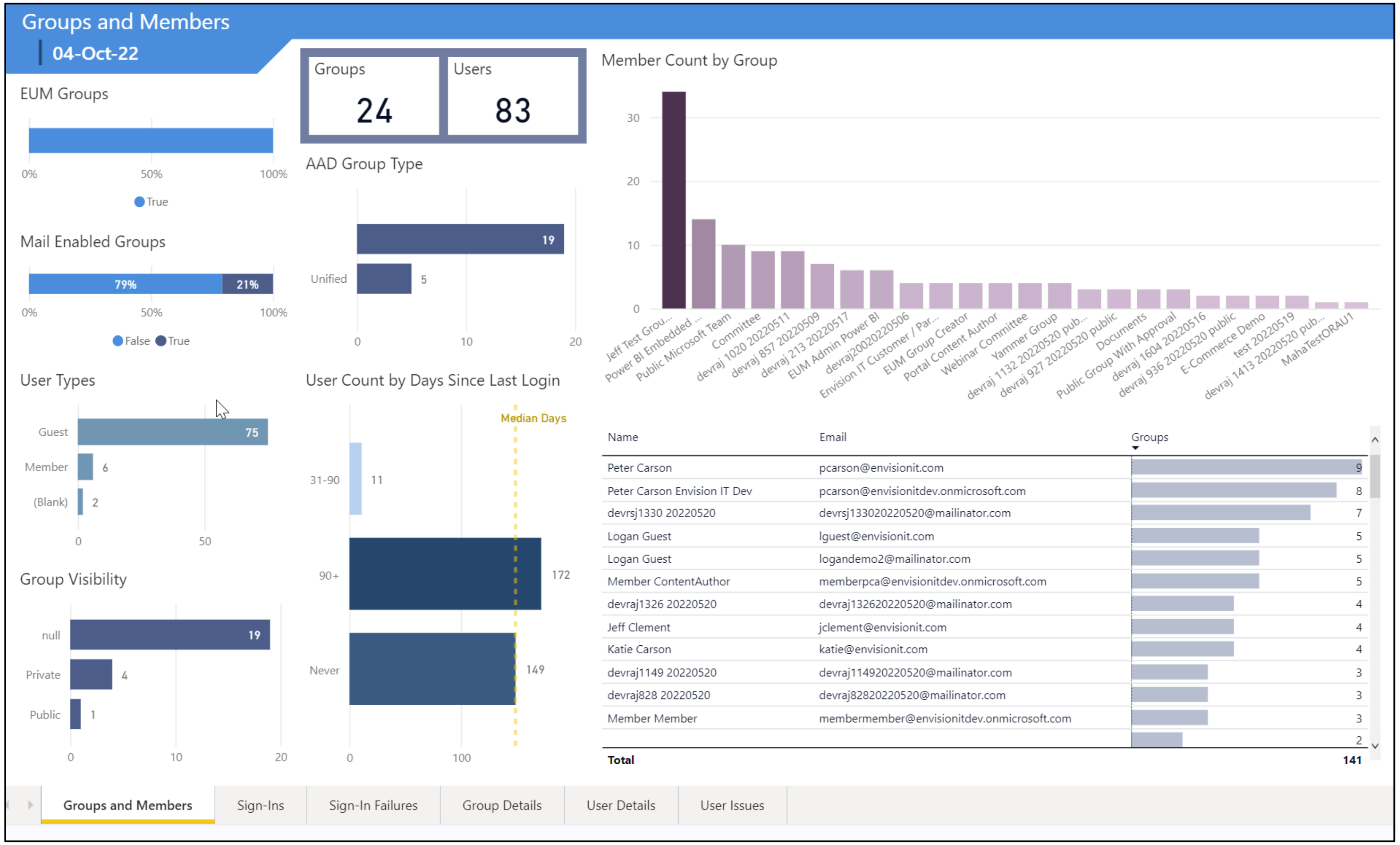
Related Assets

Configuring Azure AD B2B for External Users

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

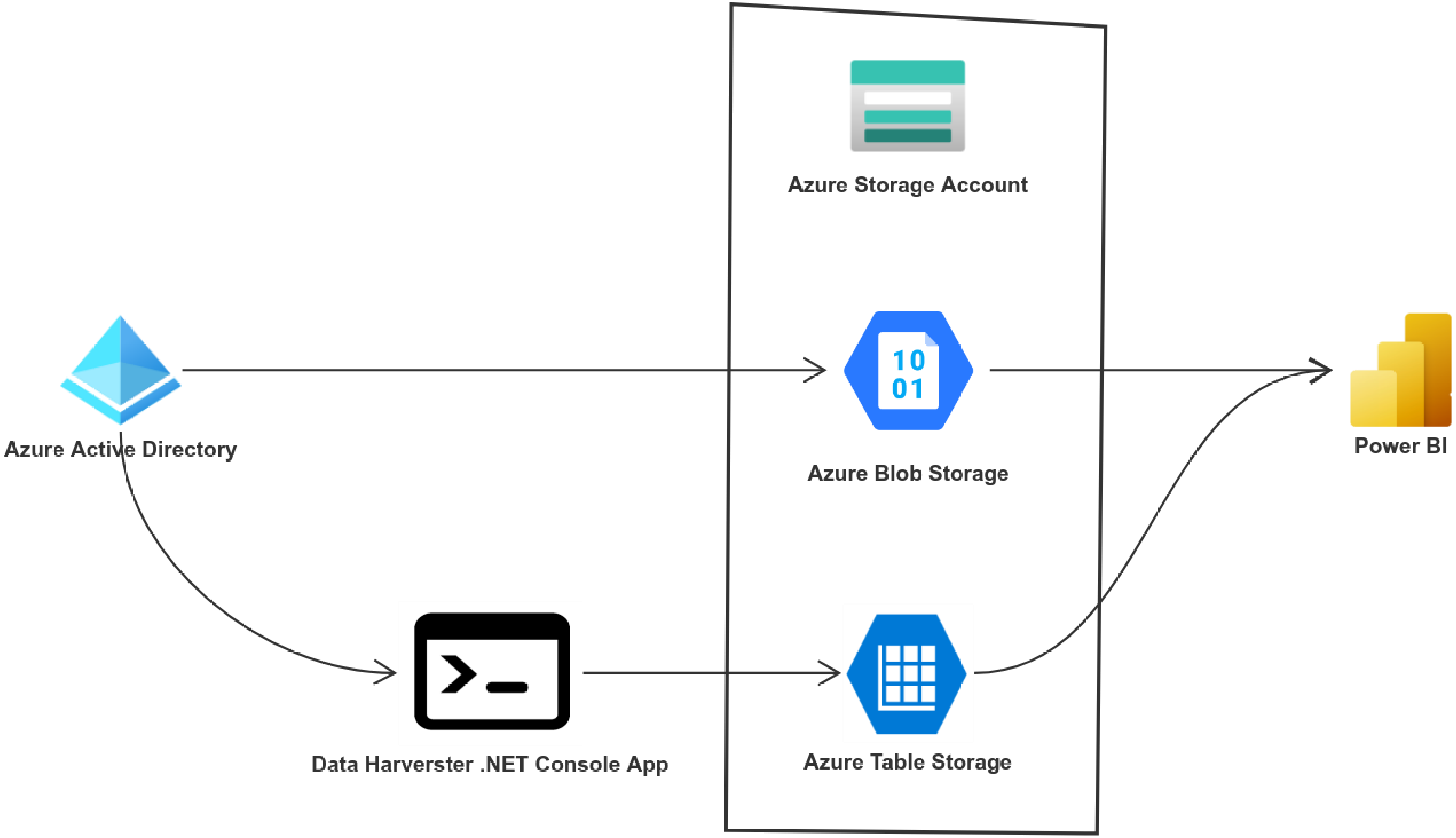
https://github.com/extranet-user-manager/EUM_AzureADPowerBI

Azure AD Power BI Dashboard



Name	Email	Groups
Peter Carson	pcarson@envisionit.com	9
Peter Carson Envision IT Dev	pcarson@envisionitdev.onmicrosoft.com	8
devrsj1330 20220520	devrsj13020220520@mailinator.com	7
Logan Guest	lguest@envisionit.com	5
Logan Guest	logandemo2@mailinator.com	5
Member ContentAuthor	memberpca@envisionitdev.onmicrosoft.com	5
devraj1326 20220520	devraj132620220520@mailinator.com	4
Jeff Clement	jclement@envisionit.com	4
Katie Carson	katie@envisionit.com	4
devraj1149 20220520	devraj114920220520@mailinator.com	3
devraj828 20220520	devraj82820220520@mailinator.com	3
Member Member	membermember@envisionitdev.onmicrosoft.com	3
		2
Total		141

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

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

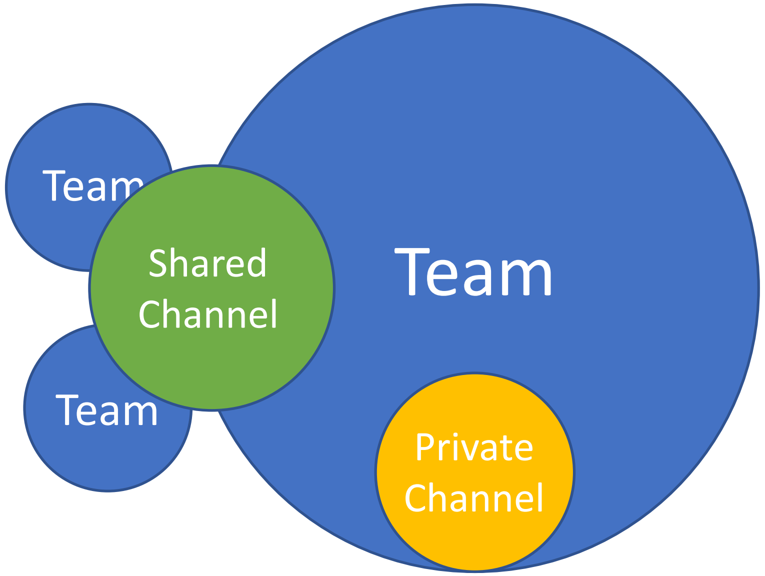
- Needs to be enabled on both tenants
    - More for organization to organization sharing
- No tenant switching
- Shared channels appear with all the home Teams and channels
- Also appear in home activity feed

How We Use Teams Shared Channels | Extranet User Manager

Shared Channels vs. Private Channels

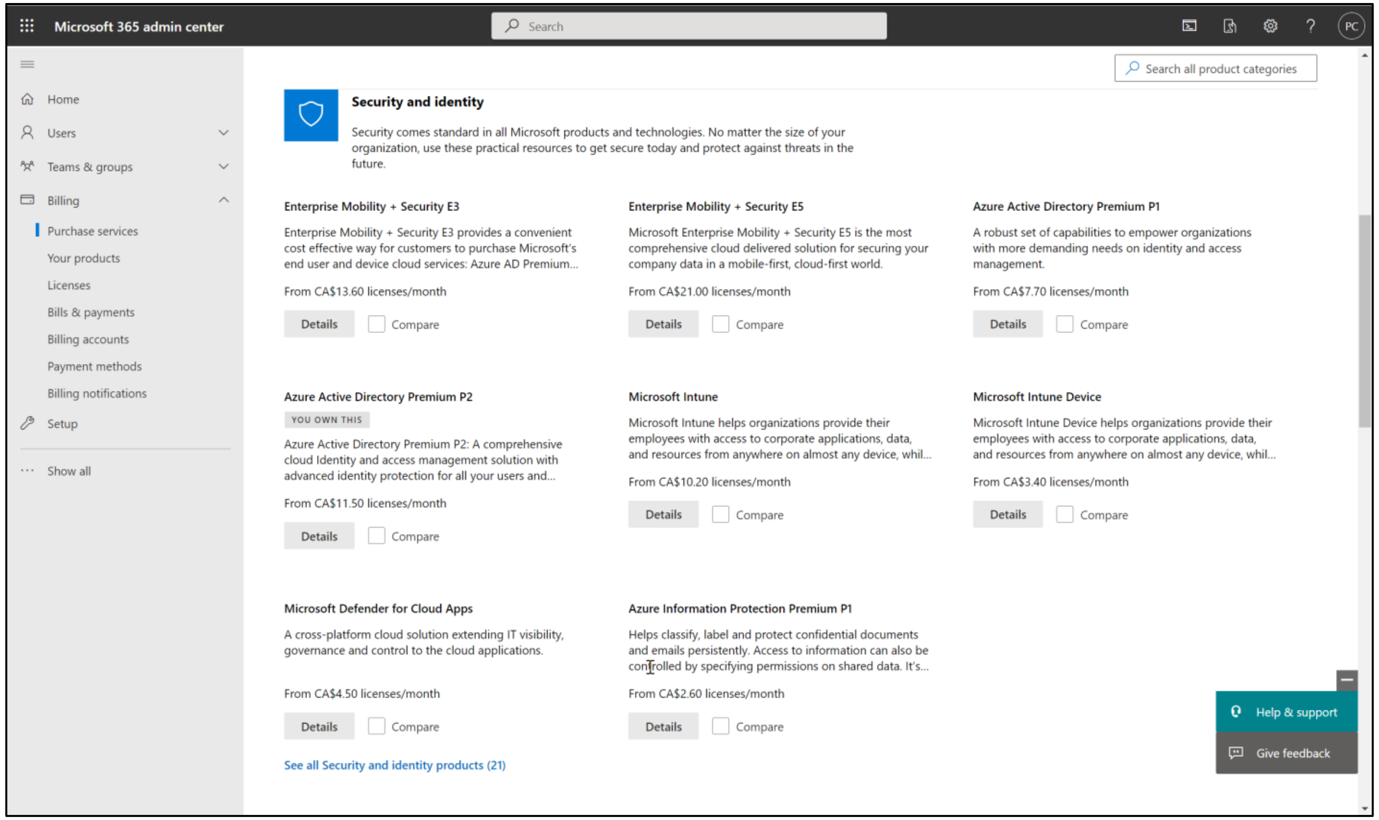
- Both channel styles create a channel site collection for documents
- Both have Teams restrictions on Apps and features
- Private channels let you invite a subset of the parent Team's members
- Shared channels let you invite anyone allowed in the tenant
  - Can also include other Teams

- 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



Licensing

Microsoft 365 Admin Center



Security and identity

Security comes standard in all Microsoft products and technologies. No matter the size of your organization, use these practical resources to get secure today and protect against threats in the future.

Enterprise Mobility + Security E3

Enterprise Mobility + Security E3 provides a convenient cost effective way for customers to purchase Microsoft's end user and device cloud services: Azure AD Premium...

From CA$13.60 licenses/month

Details □ Compare

Enterprise Mobility + Security E5

Microsoft Enterprise Mobility + Security E5 is the most comprehensive cloud delivered solution for securing your company data in a mobile-first, cloud-first world.

From CA$21.00 licenses/month

Details □ Compare

Azure Active Directory Premium P1

A robust set of capabilities to empower organizations with more demanding needs on identity and access management.

From CA$7.70 licenses/month

Details □ Compare

Azure Active Directory Premium P2

YOU OWN THIS

Azure Active Directory Premium P2: A comprehensive cloud Identity and access management solution with advanced identity protection for all your users and...

From CA$11.50 licenses/month

Details □ Compare

Microsoft Intune

Microsoft Intune helps organizations provide their employees with access to corporate applications, data, and resources from anywhere on almost any device, whil...

From CA$10.20 licenses/month

Details □ Compare

Microsoft Intune Device

Microsoft Intune Device helps organizations provide their employees with access to corporate applications, data, and resources from anywhere on almost any device, whil...

From CA$3.40 licenses/month

Details □ Compare

Microsoft Defender for Cloud Apps

A cross-platform cloud solution extending IT visibility, governance and control to the cloud applications.

From CA$4.50 licenses/month

Details □ Compare

Azure Information Protection Premium P1

Helps classify, label and protect confidential documents and emails persistently. Access to information can also be controlled by specifying permissions on shared data. It's...

From CA$2.60 licenses/month

Details □ Compare

See all Security and identity products (21)

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:

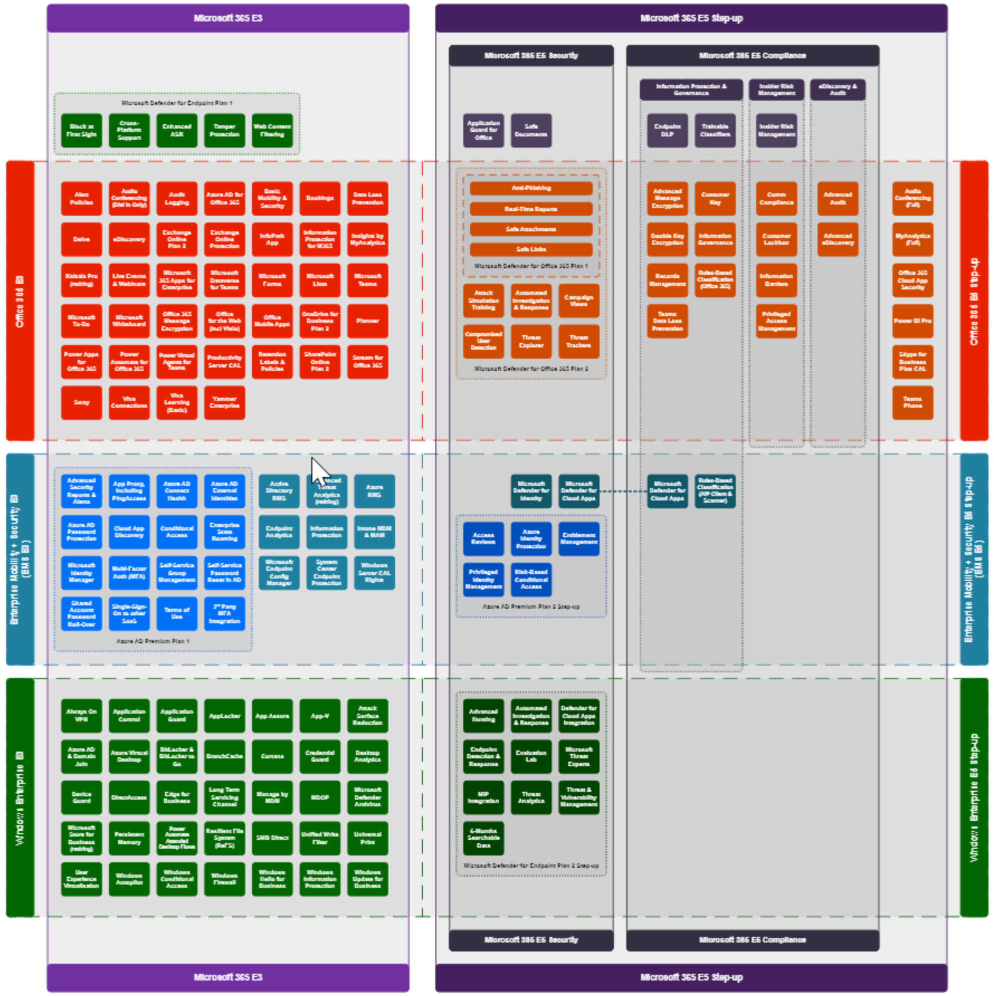
- Microsoft 365 E5/A5/G5/E3/A3/G3/F1/F3/Business Premium
- Enterprise Mobility + Security E3/E5
- AIP Plan 1
- AIP Plan 2

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

Microsoft 365 Licensing

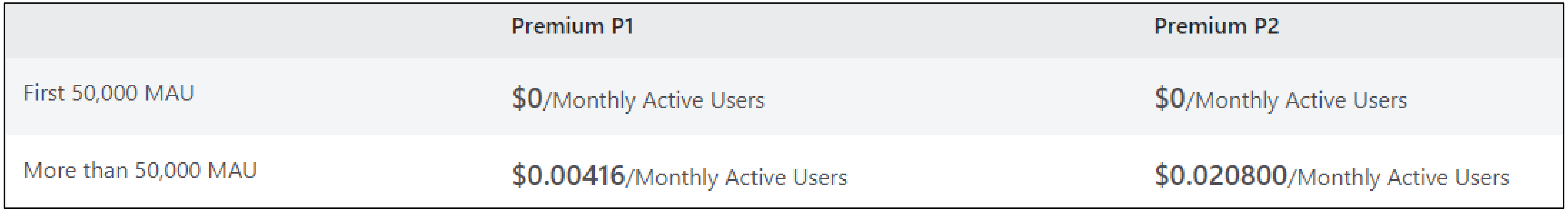
Aaron Dinnage

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


Microsoft 365 E3
Microsoft Defender for Endpoint Plan 1
Block at First Sight
Cross-Platform Support
Enhanced ASR
Tamper Protection
Web Content Filtering
Office 365 E3
Alert Policies
Audio Conferencing (Dial In Only)
Audit Logging
Azure AD for Office 365
Basic Mobility & Security
Bookings
Data Loss Prevention
Delve
eDiscovery
Exchange Online Plan 2
Exchange Online Protection
InfoPath App
Information Protection for M365
Insights by MyAnalytics
Kaizala Pro (retiring)
Live Events & Webinars
Microsoft 365 Apps for Enterprise
Microsoft Dataverse for Teams
Microsoft Forms
Microsoft Lists
Microsoft Teams
Microsoft To-Do
Microsoft Whiteboard
Office 365 Message Encryption
Office for the Web (incl Visio)
Office Mobile Apps
OneDrive for Business Plan 2
Planner
Power Apps for Office 365
Power Automate for Office 365
Power Virtual Agents for Teams
Productivity Server CAL
Retention Labels & Policies
SharePoint Online Plan 2
Stream for Office 365
Sway
Viva Connections
Viva Learning (Basic)
Yammer Enterprise
Enterprise Mobility + Security E3 (EMS E3)
Advanced Security Reports & Alerts
App Proxy, Including PingAccess
Azure AD Connect Health
Azure AD External Identities
Azure AD Password Protection
Cloud App Discovery
Conditional Access
Enterprise State Roaming
Microsoft Identity Manager
Multi-Factor Auth (MFA)
Self-Service Group Management
Self-Service Password Reset in AD
Shared Account Password Roll-Over
Single-Sign-On to other SaaS
Terms of Use
3rd Party MFA Integration
Azure AD Premium Plan 1
Active Directory RMS
Advanced Threat Analytics (retiring)
Azure RMS
Endpoint Analytics
Information Protection
Intune MDM & MAM
Microsoft Endpoint Config Manager
System Center Endpoint Protection
Windows Server CAL Rights
Windows Enterprise E3
Always On VPN
Application Control
Application Guard
AppLocker
App Assure
App-V
Attack Surface Reduction
Azure AD & Domain Join
Azure Virtual Desktop
BitLocker & BitLocker to Go
BranchCache
Cortana
Credential Guard
Desktop Analytics
Device Guard
DirectAccess
Edge for Business
Long Term Servicing Channel
Manage by MDM
MDOP
Microsoft Defender Antivirus
Microsoft Store for Business (retiring)
Persistent Memory
Power Automate Attended Desktop Flows
Resilient File System (ReFS)
SMB Direct
Unified Write Filter
Universal Print
User Experience Virtualization
Windows Autopilot
Windows Conditional Access
Windows Firewall
Windows Hello for Business
Windows Information Protection
Windows Update for Business
Microsoft 365 E3
Microsoft 365 E5 Step-up
Microsoft 365 E5 Security
Application Guard for Office
Safe Documents
Anti-Phishing
Real-Time Reports
Safe Attachments
Safe Links
Microsoft Defender for Office 365 Plan 1
Attack Simulation Training
Automated Investigation & Response
Campaign Views
Compromised User Detection
Threat Explorer
Threat Trackers
Microsoft Defender for Office 365 Plan 2
Microsoft Defender for Identity
Microsoft Defender for Cloud Apps
Access Reviews
Azure Identity Protection
Entitlement Management
Privileged Identity Management
Risk-Based Conditional Access
Azure AD Premium Plan 2 Step-up
Advanced Hunting
Automated Investigation & Response
Defender for Cloud Apps Integration
Endpoint Detection & Response
Evaluation Lab
Microsoft Threat Experts
MIP Integration
Threat Analytics
Threat & Vulnerability Management
6-Months Searchable Data
Microsoft Defender for Endpoint Plan 2 Step-up
Microsoft 365 E5 Security
Microsoft 365 E5 Compliance
Information Protection & Governance
Insider Risk Management
eDiscovery & Audit
Endpoint DLP
Trainable Classifiers
Insider Risk Management
Advanced Message Encryption
Customer Key
Comm Compliance
Advanced Audit
Double Key Encryption
Information Governance
Customer Lockbox
Advanced eDiscovery
Records Management
Rules-Based Classification (Office 365)
Information Barriers
Teams Data Loss Prevention
Privileged Access Management
Microsoft Defender for Cloud Apps
Rules-Based Classification (AIP Client & Scanner)
Microsoft 365 E5 Compliance
Audio Conferencing (Full)
MyAnalytics (Full)
Office 365 Cloud App Security
Power BI Pro
Skype for Business Plus CAL
Teams Phone
Office 365 E5 Step-up
Enterprise Mobility + Security E5 Step-up (EMS E5)
Windows Enterprise E5 Step-up
Microsoft 365 E5 Step-up

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)
- Internal employee users are not eligible
  - Consider Microsoft 365 F1

Thank you!

Questions?