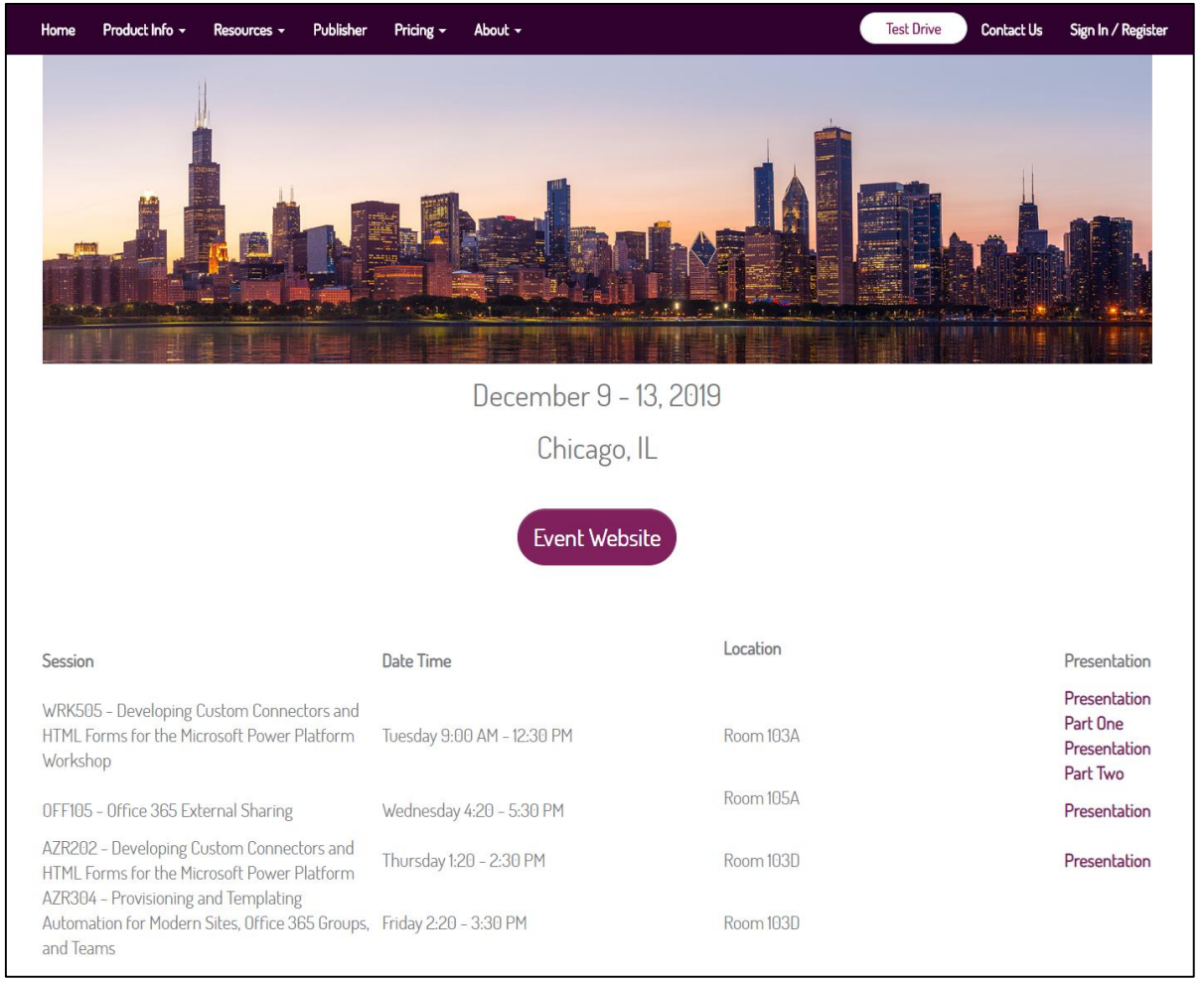
Office 365 External Sharing

Wednesday, December 11, 2019

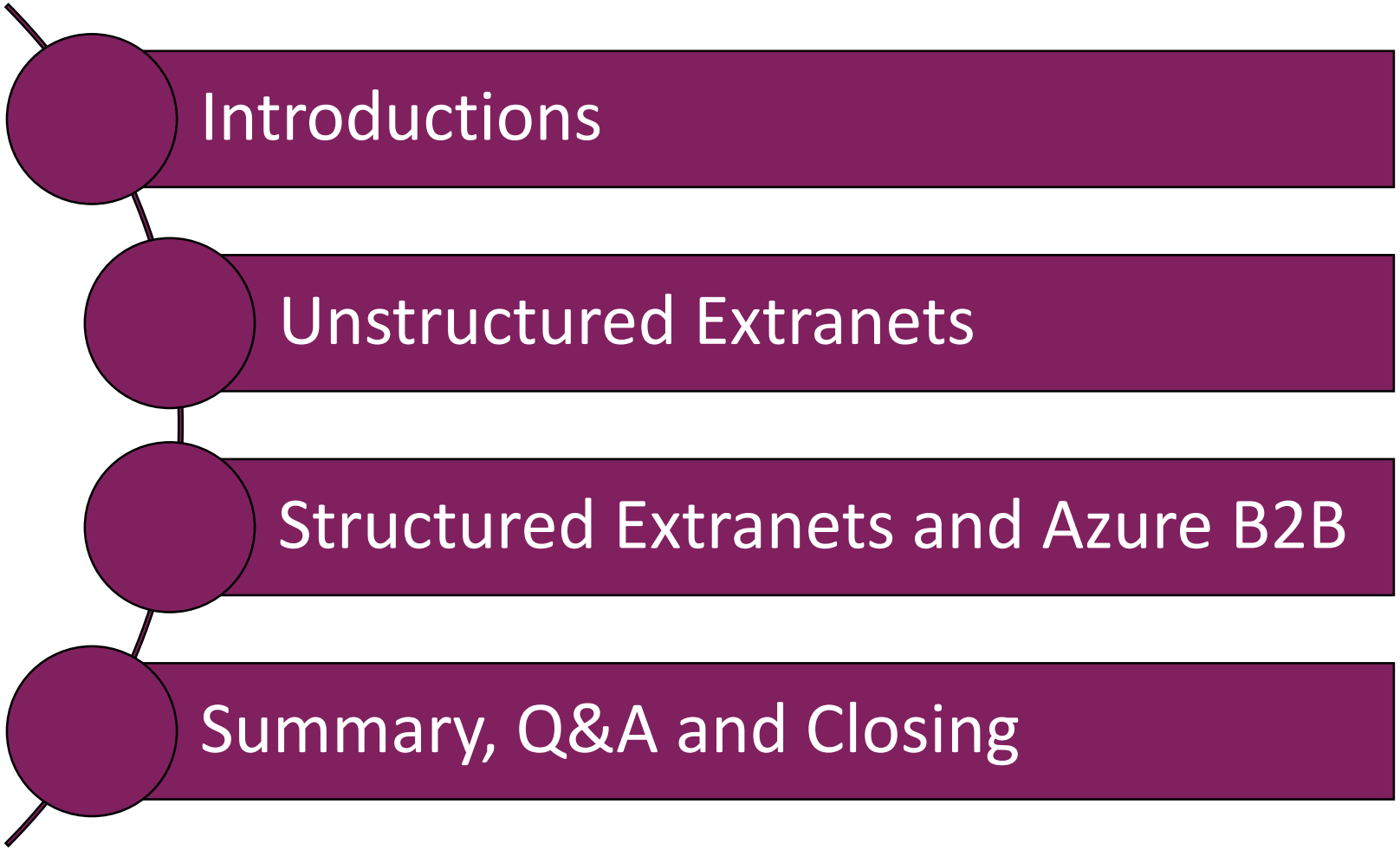
Peter Carson

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

http://eum.co/resources/events



Agenda


Introductions
Unstructured Extranets
Structured Extranets and Azure B2B
Summary, Q&A and Closing

Poll – Which do you use today?

Office 365

Microsoft 365

Enterprise Mobility + Security

Azure AD Premium P1 or P2

Styles of Extranets

Collaborative

- **Unstructured or structured**
- **SharePoint Online (Office 365) or on premises**
- **Collaborating on documents**
  - File upload and download
  - Editing
  - Various file types
- **Often project focused**

Publishing

- **One to many**
- **Typically structured**
- **Secure website**
- **May also have a public (anonymous) section**
- **Self-registration is common**
- **One way push of private content out**
- **Limited feedback**
  - Like and comment
  - File upload
- **Profile management**

Five Considerations for your Extranet

1. **Who will be accessing the extranet? Is there a member database to interface with?**

- Members
- Customers
- Vendors
- Suppliers
- Volunteers
- Board of Directors
- Citizens
- Researchers
- Tenants
- Partners

Five Considerations for your Extranet

1. Who will be accessing the extranet? Is there a member database to interface with?
2. **Self-registration option or invitation only? Who approves new registrations?**

Invitation Only

- Smaller, known set of users
- Private registration links can be shared with potential users
- Managed centrally or delegated

Self Registration

- Onboarding hundreds or thousands of external users
- Approval workflows
- Auto-approvals
- Delegation

Five Considerations for your Extranet

1. Who will be accessing the extranet? Is there a member database to interface with?
2. Self-registration option or invitation only? Who approves new registrations?
3. **How will your extranet users authenticate?**

- Email and password
  - Self-service password reset
- Office 365 / Azure AD
- Microsoft Account
- Google
- Facebook
- LinkedIn
- Twitter

Five Considerations for your Extranet

1. Who will be accessing the extranet? Is there a member database to interface with?
2. Self-registration option or invitation only? Who approves new registrations?
3. How will your extranet users authenticate?
4. **What interactions are your external users going to have?**

- Accessing published content
- Collaborating on specific documents
- Accessing team or project sites
- Becoming full-fledged members of Office 365 Groups or Teams

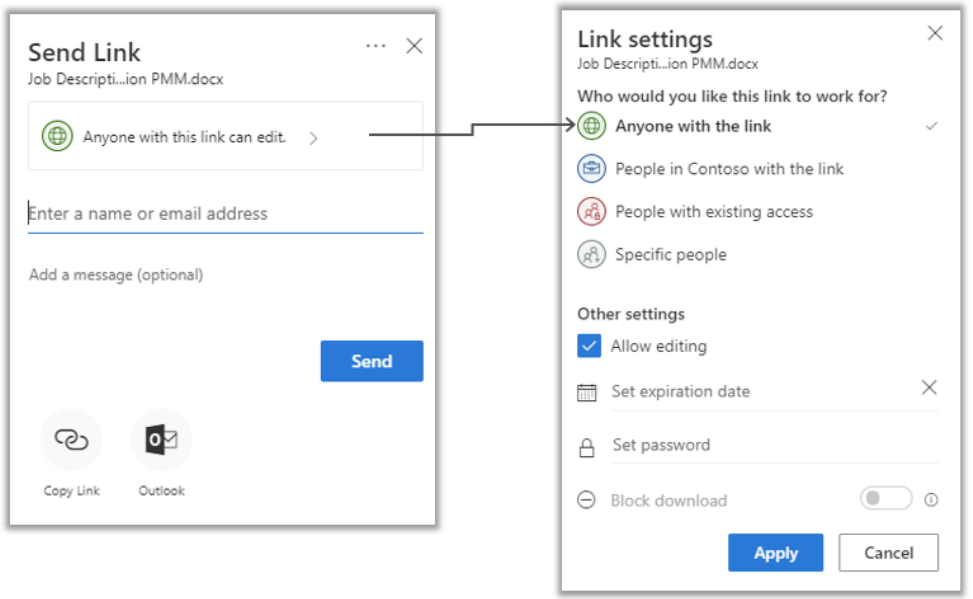
Five Considerations for your Extranet

1. Who will be accessing the extranet? Is there a member database to interface with?
2. Self-registration option or invitation only? Who approves new registrations?
3. How will your extranet users authenticate?
4. What interactions are your external users going to have?
5. **What applications will be accessible?**

- Office 365 - SharePoint Online, OneDrive for Business
- Office 365 Groups – Teams, Planner, Yammer
- Other Office 365 Apps - Power BI, Stream, PowerApps, Flow
- SharePoint On Premises
- Third Party SaaS Applications
- Custom Applications – On Premise or Cloud

Unstructured Extranets with Office 365 External Sharing

- **External Sharing in Office 365 strongly supports ad-hoc collaboration**
- **Sharing documents with a few to a few dozen external people**
- **Secure Link sharing to sites, libraries, and documents**
  - Anyone with the link (Anonymous)
  - People in your Organization
  - People with existing access
  - Specific people



Office 365 External Sharing OOTB

1. Who will be accessing the extranet?
2. Self-registration option or invitation only?
3. How will your extranet users authenticate?
4. What interactions are your external users going to have?
5. What applications will be accessible?

1. Any type of external user
2. Invitation only
3. Office 365 / Azure AD, Microsoft Account, One Time Passcode, Gmail
4. Any interactions
5. Office 365 only

Admin controls for external sharing

Managing external sharing

Control WHO can share to external users

- Everyone
- Only specific people
- No one

Control WHICH external users can be shared with

- Anyone
- Only authenticated users
- Only authenticated users except specific domains
- Only authenticated users in specific domains
- No one

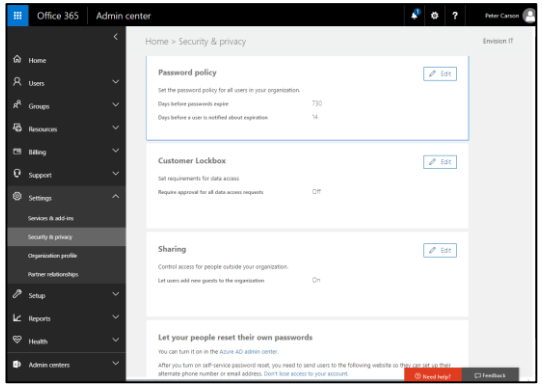
Control WHAT can be shared externally

- Anything
- Only specific sites
- Only files without sensitive content

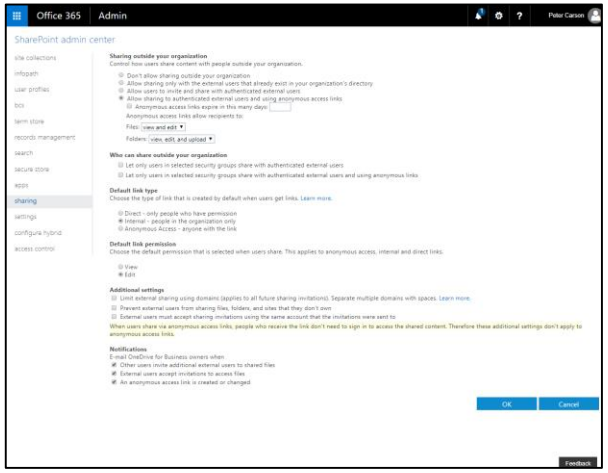
Control HOW externally shareable links can be used

- Default
- Enabled, but not default
- Mandatory expiration date
- Block externally-shareable edit links
- Disabled

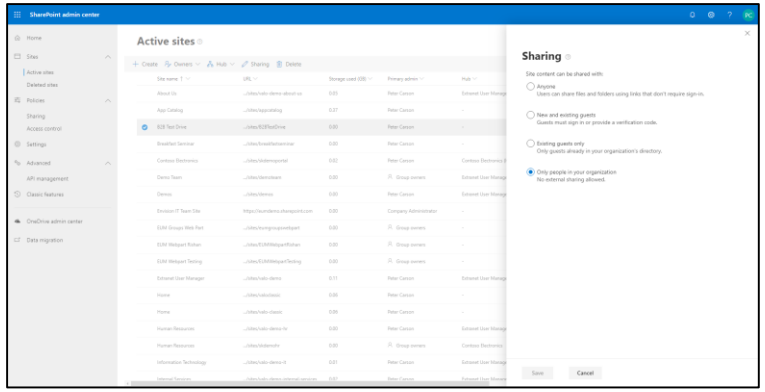
Three Places to Configure External Sharing



Office 365 Admin



SharePoint Admin



Site Collection Admin

PowerShell

Scenario: simple external sharing

I’m sending sales materials to a customer

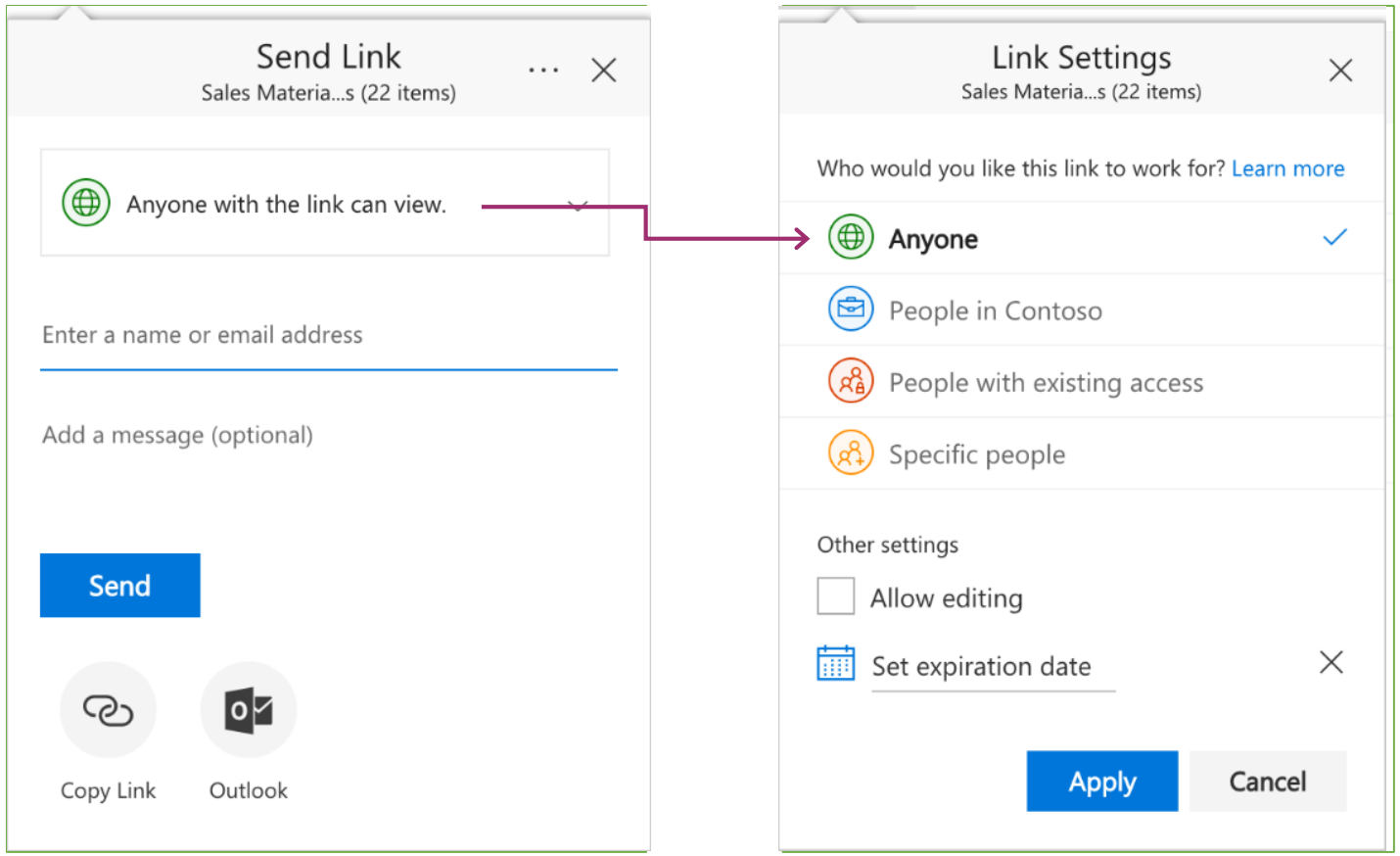
Make it **easy** for them

Don’t make them sign-in

Don’t make them create an account

Let them forward it to whoever they want

Shareable Links



- Link works for anyone who has it
- Like an attachment
- Can be read-only or editable
- Can set an expiration date
- Recipients decide who else gets access
- Guaranteed to open for anyone who receives it, on any device
- Share with anyone easily via email, chat, social, etc. No frustrating errors or sign-in/up

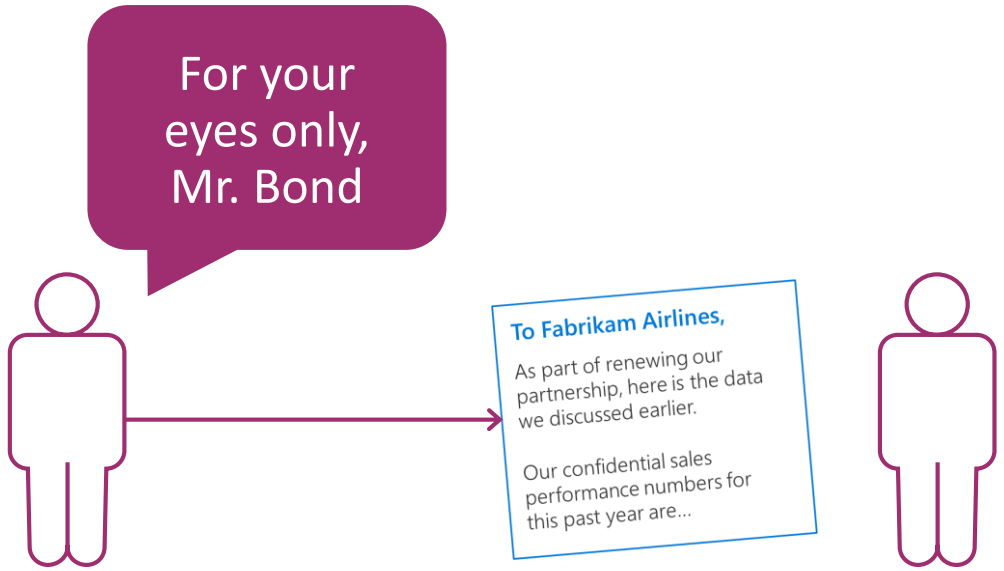
Scenario: Secure External Sharing

- **I want an external partner to review my secret document**

To Fabrikam Airlines,

As part of renewing our partnership, here is the data we discussed earlier.

Our confidential sales performance numbers for this past year are…



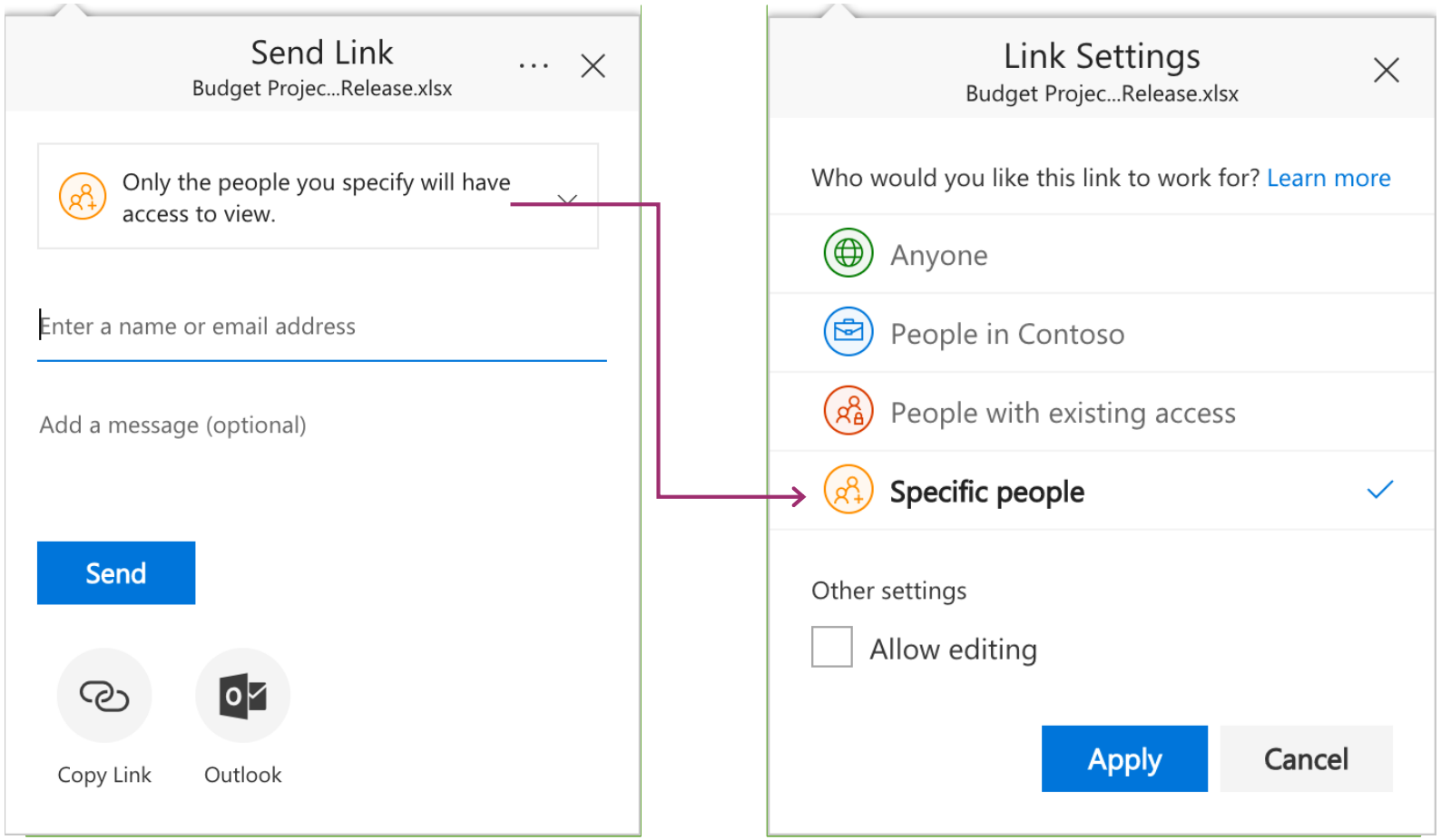
Make it **easy** for them

Minimize effort to open the link

Keep it **secure**

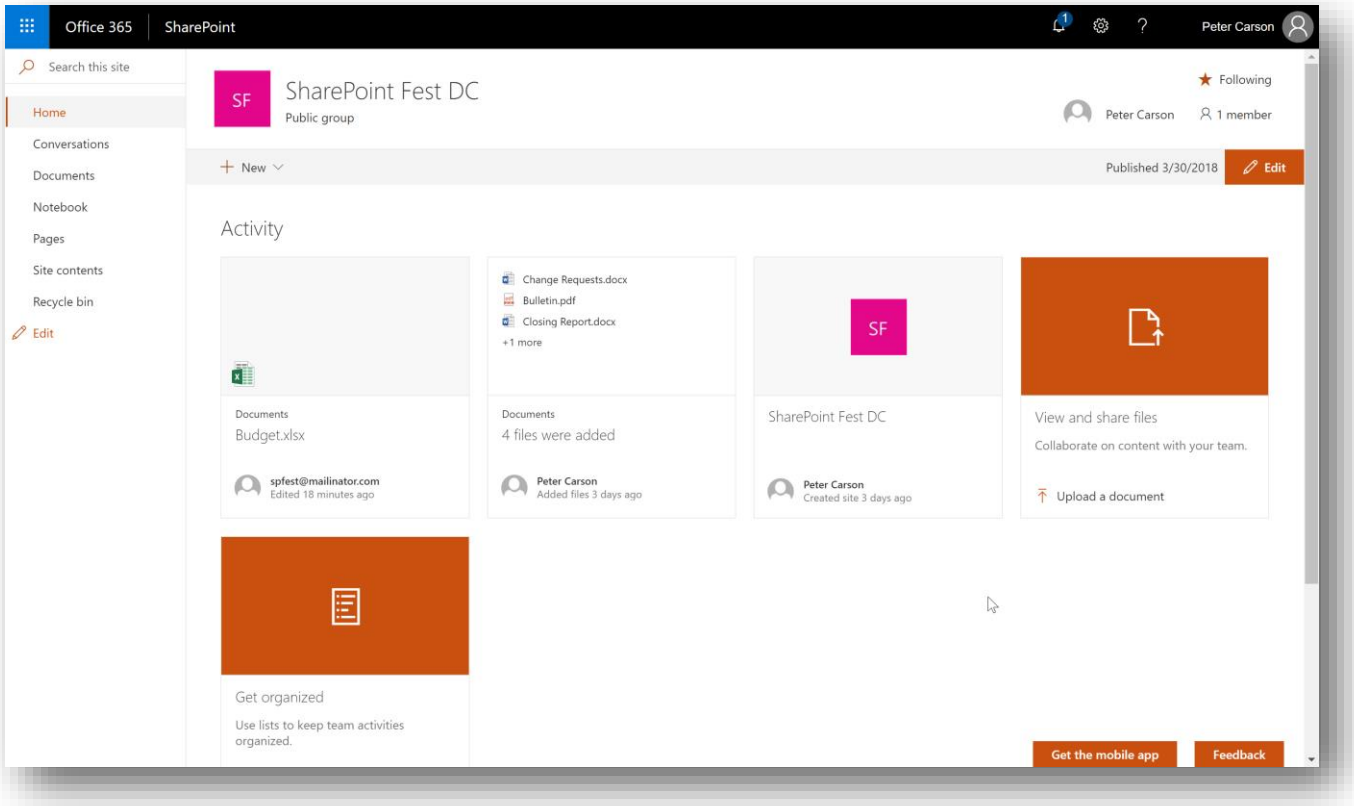
Don't let them forward it to anyone else

How to:



- Send a link that works for only specific people
- A non-transferable, revocable secret key
- Users must prove they're the intended recipient
- Internal users must be signed in to their existing account
- External users verify with a one-time passcode

External Sharing at the Site Level



- Invite external users or groups at the site, list, or library level
- Managed through regular SharePoint permissions
- External users need to sign in

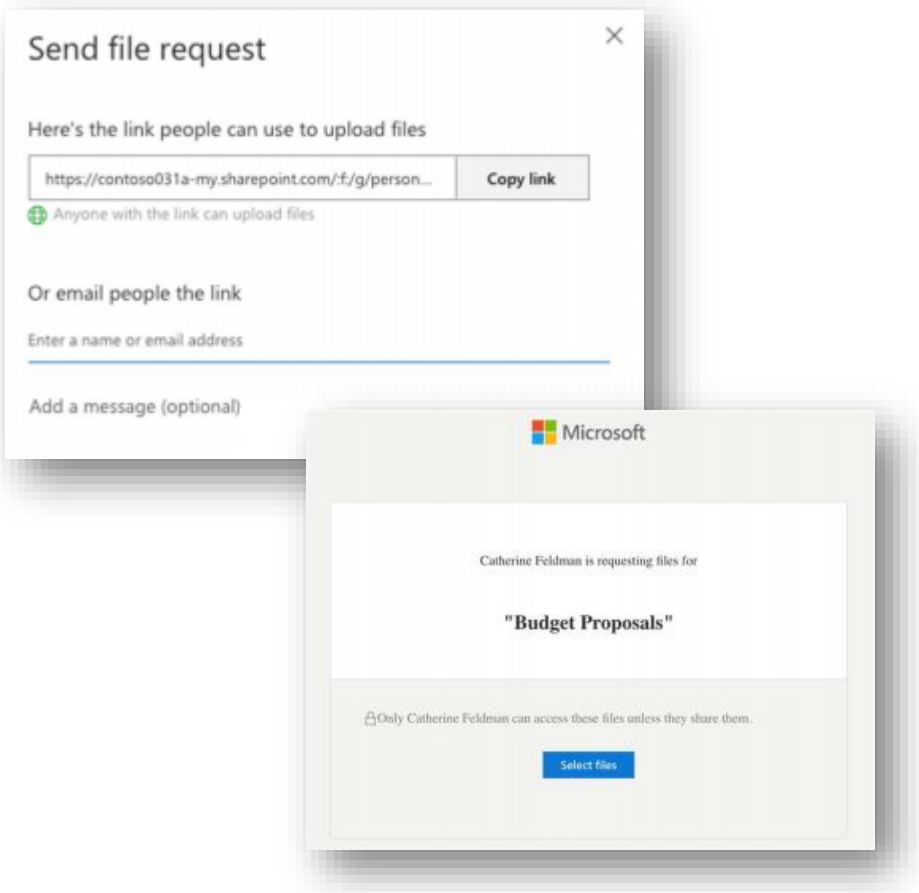
Making the News!

Exclusive interview with Mark Kashman and Stephen Rice of the Microsoft SharePoint Team

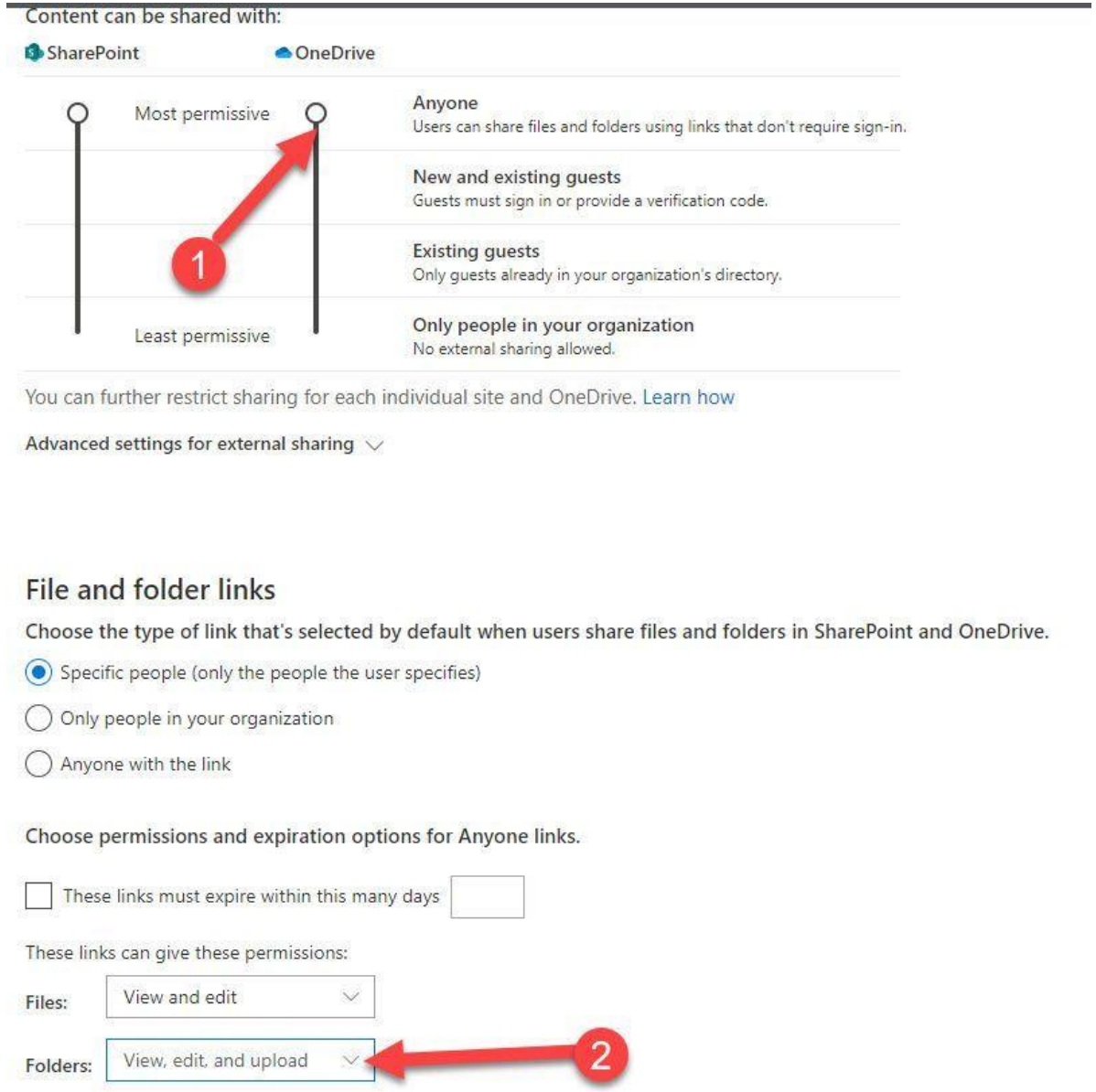
eum.co/resources/articles/external-sharing-interview-with-the-sharepoint-product-team

New External Sharing Announcements from SPC 2019

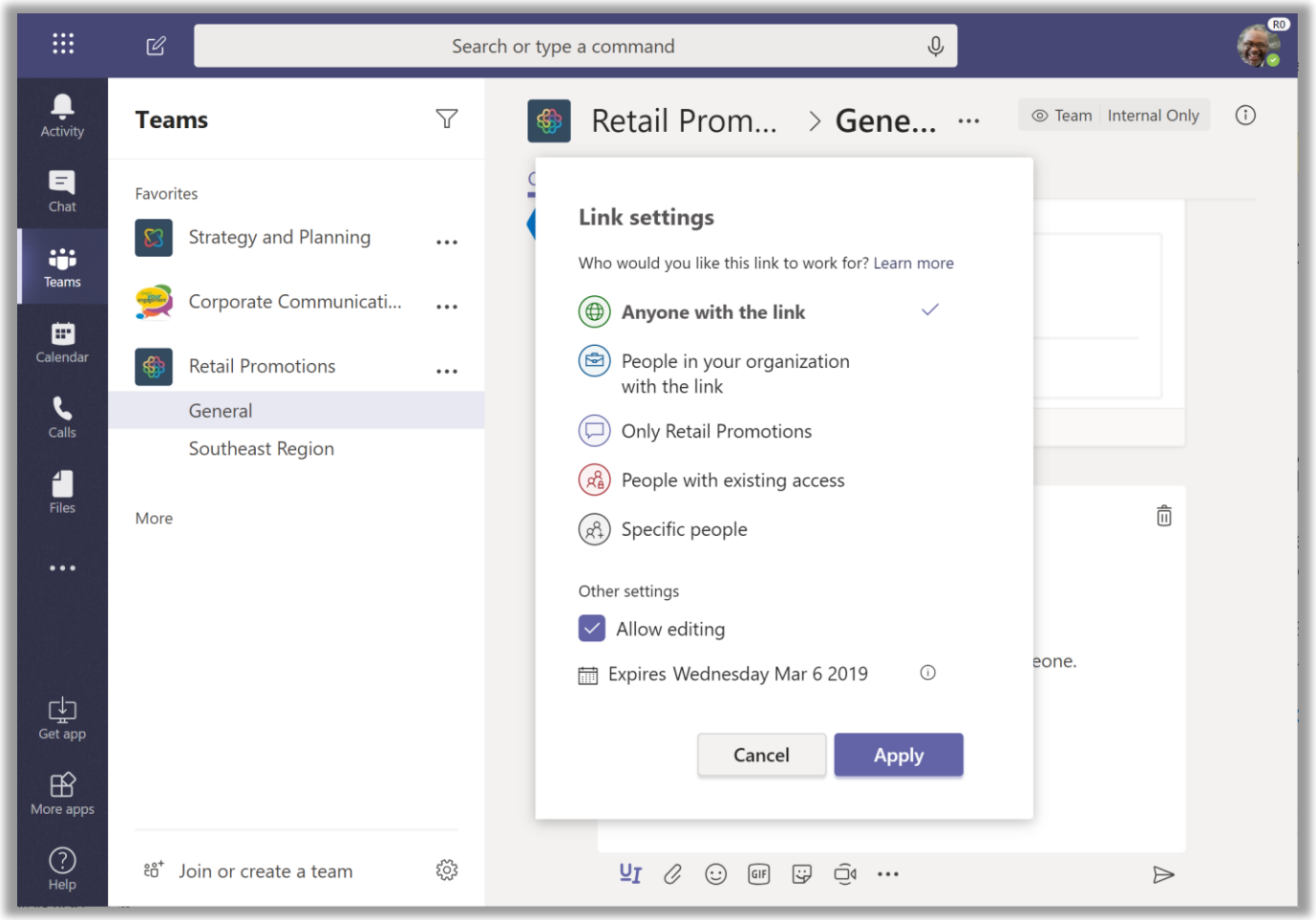
- **Request Files**
  - Ask colleagues and external guest users to upload files to a folder
  - Uploaders can only see their own content
  - Single link can be used for many uploaders



eum.co/resources/articles/external-sharing-announcements


Content can be shared with:
SharePoint
OneDrive
Most permissive
Least permissive
1
Anyone
Users can share files and folders using links that don't require sign-in.
New and existing guests
Guests must sign in or provide a verification code.
Existing guests
Only guests already in your organization's directory.
Only people in your organization
No external sharing allowed.
You can further restrict sharing for each individual site and OneDrive. Learn how
Advanced settings for external sharing
File and folder links
Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive.
Specific people (only the people the user specifies)
Only people in your organization
Anyone with the link
Choose permissions and expiration options for Anyone links.
These links must expire within this many days
These links can give these permissions:
Files:
View and edit
Folders:
View, edit, and upload
2

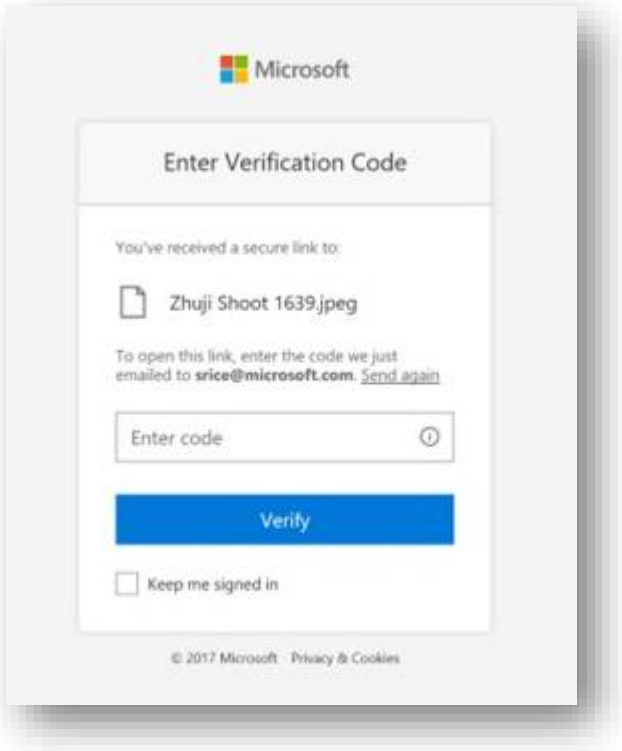
NEW! OneDrive sharing in Microsoft Teams



- Complete set of sharing features in Teams
- Share files without creating unintended copies
- Easily create links that only work for people in your team
- Follows all admin settings and policies you've configured
- Coming soon

New External Sharing Announcements from SPC 2019

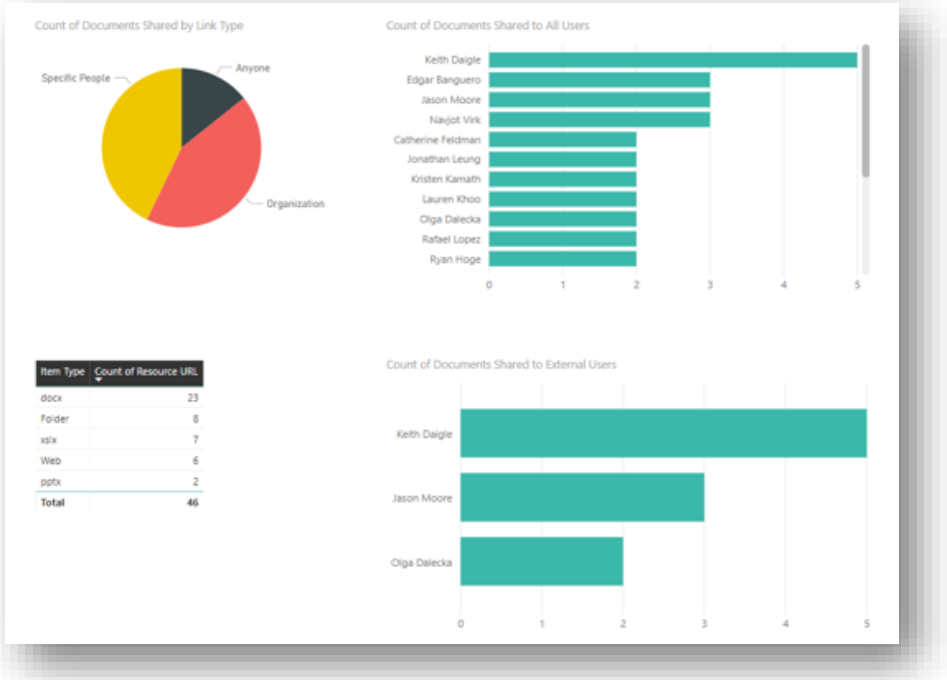
- **Deeper Integration with Azure AD B2B**
  - External users can sign in with One Time Passcode (OTP) to verify they own the email address
  - Able to utilize premium Azure AD functionalities
    - Conditional access
    - Multi-Factor Authentication
    - Google auth federation



eum.co/resources/articles/external-sharing-announcements

New External Sharing Announcements from SPC 2019

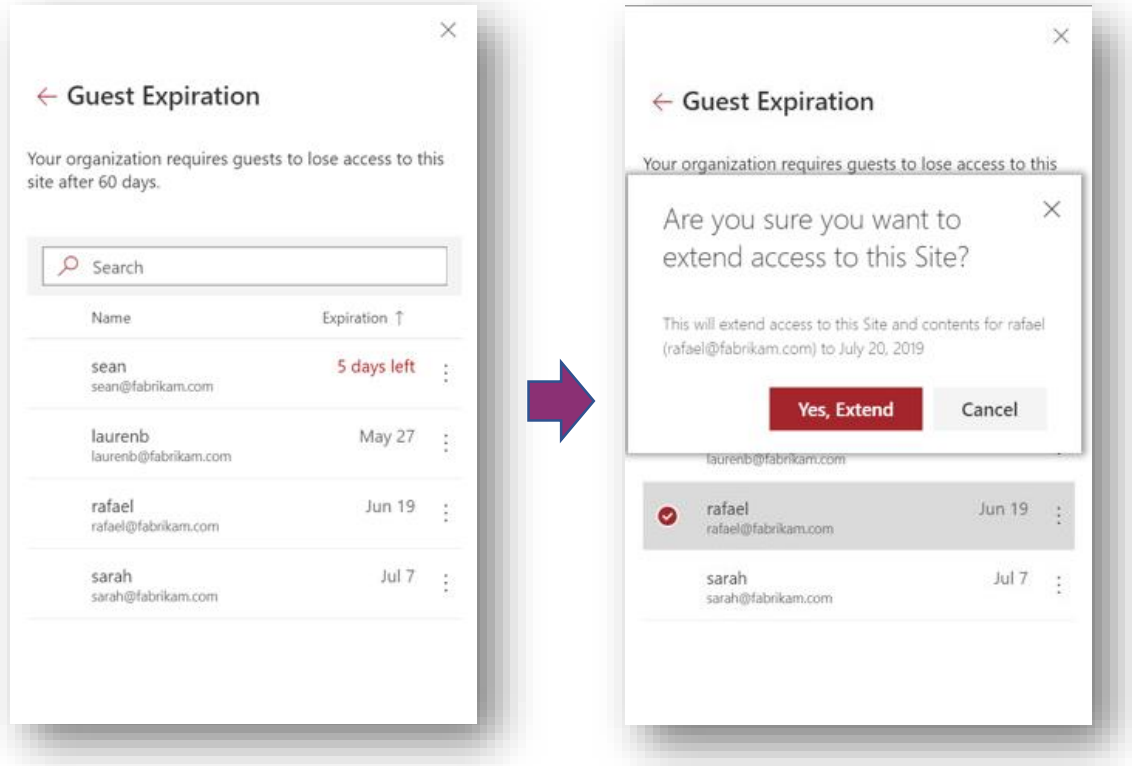
- **Enhanced Sharing Reports**
  - Access a list of unique permissions on a given site collection
  - Export report to a csv. file and import into PowerBI or Excel to build sharing dashboards
  - Go to Site Usage from the Gear menu
  - Link to Run Report



eum.co/resources/articles/external-sharing-announcements

New External Sharing Announcements from SPC 2019

- **Expiring external access**
  - Site admins can define how long a guest user has access to site contents
  - IT access policy defined at the organization level (ie. All users will lose access after 60 days)
  - Site admin can extend access for users expirations if additional time is permitted



eum.co/resources/articles/external-sharing-announcements

Securing Your Staff

You can't secure your Extranet

if your staff don't work securely

Office 365 Security Best Practices

1. Set up multi-factor authentication
2. Train your users
3. Use dedicated admin accounts
4. Raise the level of protection against malware in mail
5. Protect Against Ransomware
6. Stop auto-forwarding for email
7. Use Office Message Encryption
8. Protect your email from phishing attacks
9. Protect against malicious attachments and files with ATP Safe Attachments
10. Protect against phishing attacks with ATP Safe Links

https://docs.microsoft.com/en-us/office365/admin/security-and-compliance/secure-your-business-data?view=o365-worldwide

Microsoft

How Microsoft uses Identity Protection and Conditional Access to protect its assets

Caleb Baker
Principal PM
@caleb_b

Sarah Handler
Program Manager II
@sarahhandler

Sarah Scott
Principal PM Manger

BRK2132

ExtranetUserManager

730,000+

Compromised accounts due to password spray
in the last 4 months

67%

Reduction in account compromise when MFA is enabled

Devising our protection plan

1

Passwords are weak

Continue to require MFA for modern authentication.

2

Close the backdoor

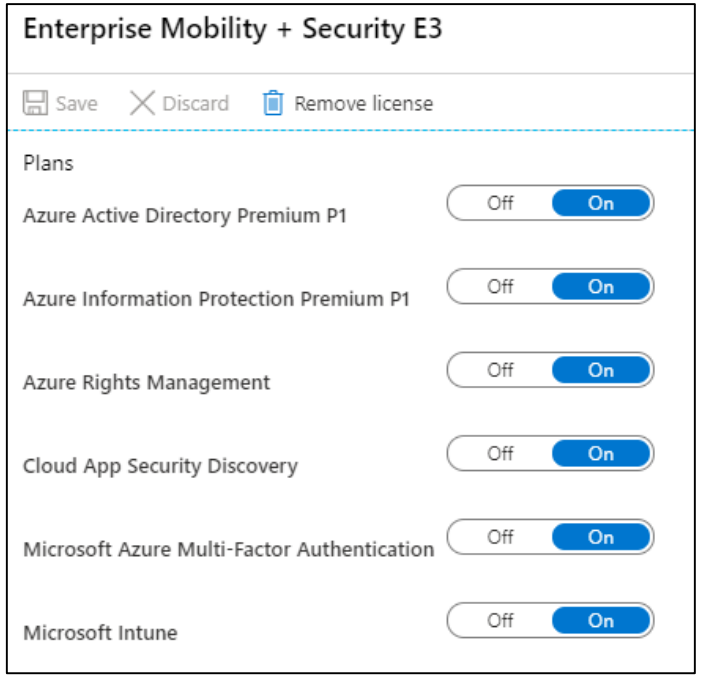
Apps not capable of MFA will be blocked.

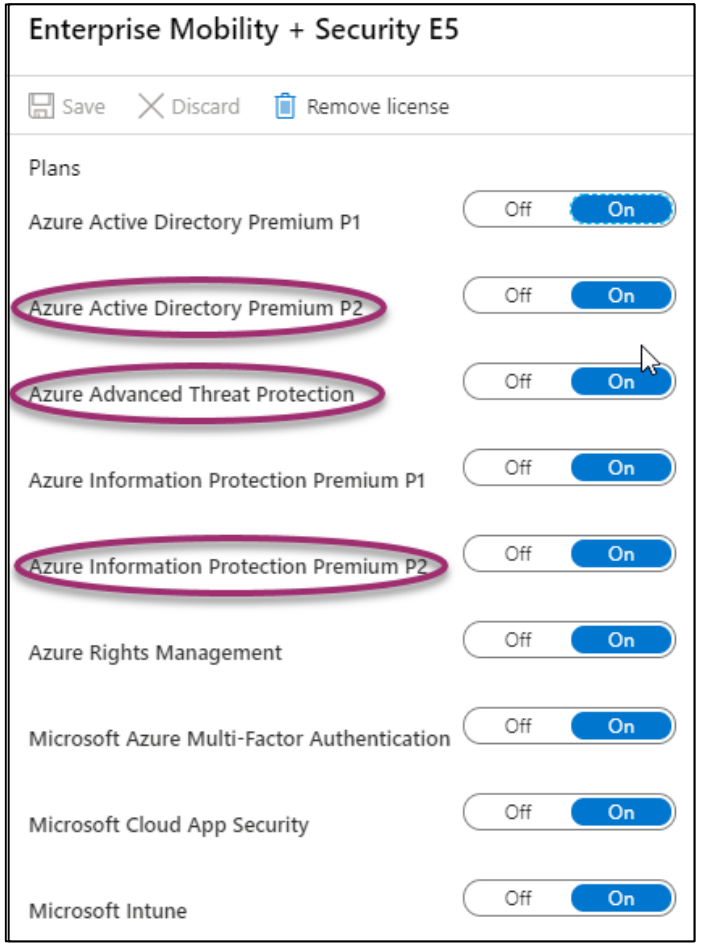
3

Fix compromised accounts

Detect compromised accounts with Azure Identity Protection. Policy forces password change on risky users.

EMS E3 vs. E5


Enterprise Mobility + Security E3
Save
Discard
Remove license
Plans
Azure Active Directory Premium P1
Off
On
Azure Information Protection Premium P1
Off
On
Azure Rights Management
Off
On
Cloud App Security Discovery
Off
On
Microsoft Azure Multi-Factor Authentication
Off
On
Microsoft Intune
Off
On


Enterprise Mobility + Security E5
Save
Discard
Remove license
Plans
Azure Active Directory Premium P1
Off
On
Azure Active Directory Premium P2
Off
On
Azure Advanced Threat Protection
Off
On
Azure Information Protection Premium P1
Off
On
Azure Information Protection Premium P2
Off
On
Azure Rights Management
Off
On
Microsoft Azure Multi-Factor Authentication
Off
On
Microsoft Cloud App Security
Off
On
Microsoft Intune
Off
On

Azure AD P1 vs. P2

Azure AD Premium P1

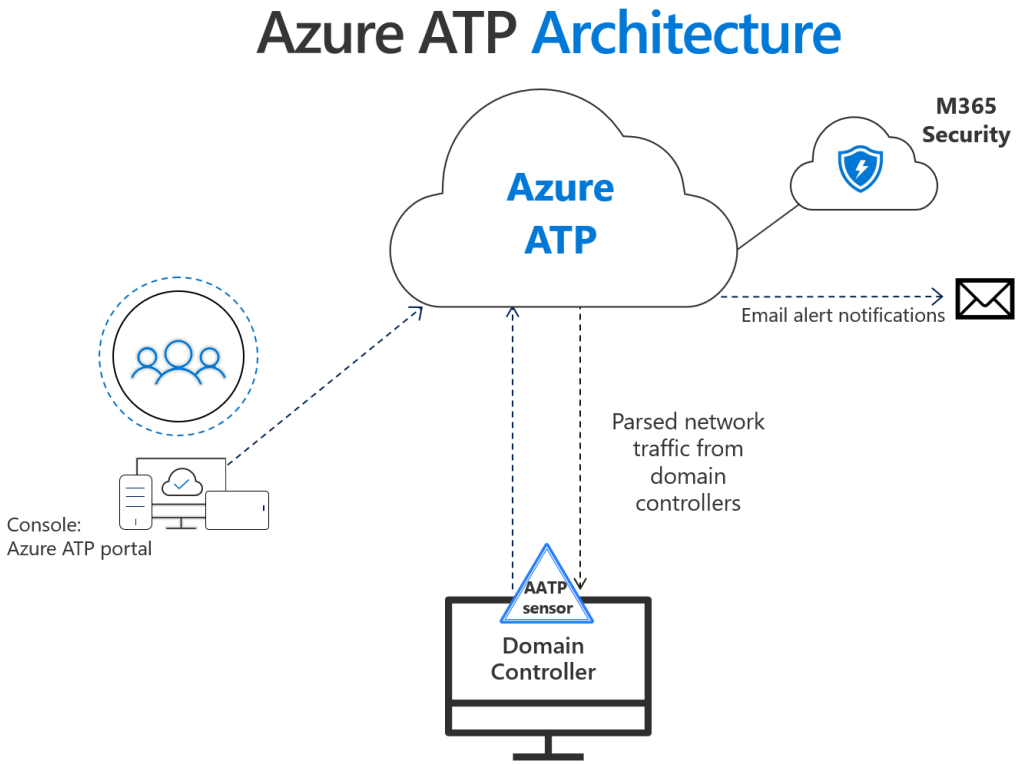
- Multi-factor authentication with Conditional Access
- Hybrid Identities
- Password protection (custom banned passwords)
- Advanced Security and Usage Reports
- Conditional Access based on group, location, and device status
- AIP integration
- And Much More

Azure AD Premium P2

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

Azure Advanced Threat Protection (ATP)

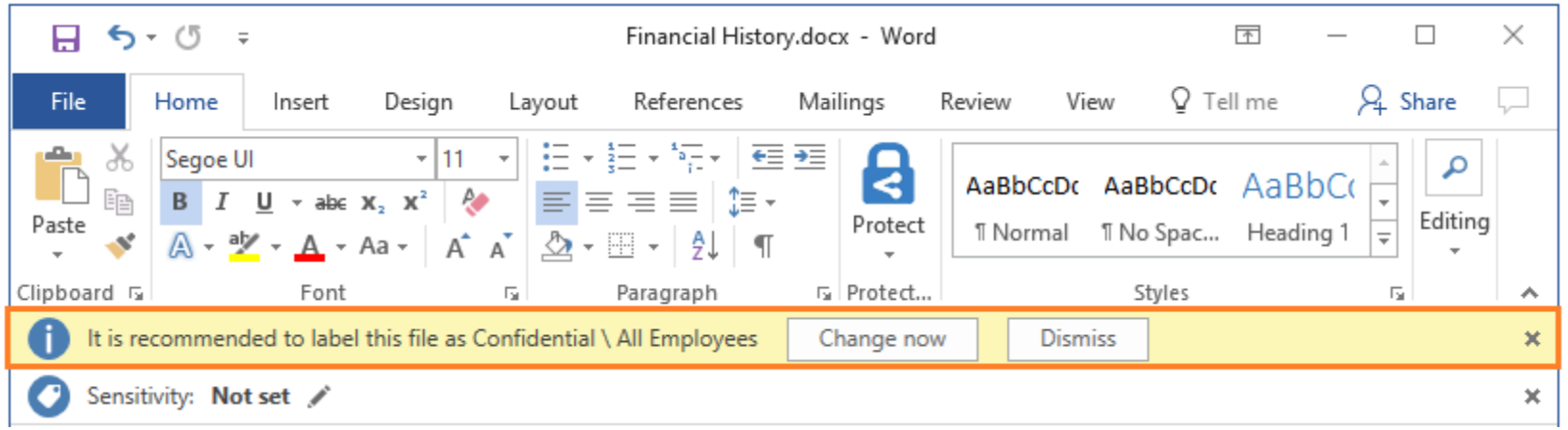
- Cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
- Monitor users, entity behavior, and activities with learning-based analytics
- 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



https://docs.microsoft.com/en-us/azure-advanced-threat-protection/what-is-atp

Azure Information Protection (AIP)

- Cloud-based solution that helps an organization to classify and protect its documents and emails by applying labels
- Labels can be applied automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations
- Uses Azure Rights Management - protection that is applied by using Rights Management stays with the documents and emails, independently of the location—inside or outside your organization, networks, file servers, and applications.



https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

Layering Up Your Security Implementation

1. **MFA is the most important feature you can turn on**
   - Office 365 provides basic MFA which prompts on every login
   - Conditional access lets you define rules for MFA
     - Managed versus unmanaged device
     - Risk level
     - Locations
     - Apps
2. **Azure Information Protection can classify content**
   - Can be used with Conditional Access to determine policy
   - Can be manually or automatically applied
3. **Advanced Threat Protection can help secure your on-premise environment**

Microsoft Security Licensing Options

- **Purchase as part of a bundle**
  - Microsoft 365 E3 or E5
    - Superset of Office 365 E3 or E5
  - Enterprise Mobility + Security E3 or E5
    - Bundled into Microsoft 365
- **Individual step up plans**
  - Azure AD Premium P1 or P2
  - Azure Advanced Threat Protection
  - Azure Information Protection P1 or P2
  - Azure Rights Management
  - Cloud App Security
  - Intune

Office 365 MFA is included in all Office 365 subscriptions

Microsoft

Securing SharePoint and OneDrive with Labels and Access Policies

Sesha Mani
Principal Group Program Manager (GPM)

/in/seshamani
@SeshaManiS

Sanjoyan Mustafi
Senior Program Manager

BRK3007

Roadmap: Security & Compliance in SharePoint & OneDrive

Available soon

Sensitivity Labels

- Sensitivity labels for Sites and Office 365 Groups (Public Preview)
- Sensitivity labels with Protection for Files (Public Preview)
- **SPO Auto Classification with Sensitivity Labels** (Private Preview)

Policies

- Automatic expiration of external user access (GA)
- DLP block external access by default for SharePoint (GA)

Compliance

- **Information Barriers** (Private Preview)

Sign-up for private previews at:
https://aka.ms/ODSPSecurityPreviews

Learn more at:
https://aka.ms/ODSPSecurity19

Early next year

- DLP block anonymous access for sensitive files (GA)
- Sensitivity labels for Sites and Office 365 Groups (GA)
- Sensitivity labels with Protection for Files (GA)
- **SPO Auto Classification with Sensitivity Labels** (GA)

Top of mind

- **Granular conditional access at site level with MFA (Multi-factor-authentication)**
- **Office 365 unified instant access revocation**
- **Conditional access for Office 365 App Group**

Structured Extranets

- **Typically hundreds to thousands of external users**
- **Represent many different groups of external users**
  - Projects
  - Committees
  - Customers
  - Vendors
  - Partners
- **May be many different business owners**
  - Owners can be internal or external

When to use….

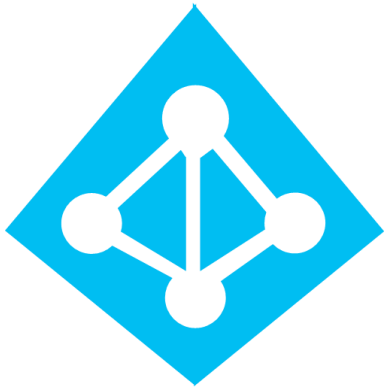
External Sharing

- Sharing with a few people
- Co-authoring on individual documents
- You are the sole administrator of permissions
- Eliminate the use of other shadow IT within the organization

EUM with Azure AD B2B

- Sharing with many people with granular permission sets
- Self service functionalities like Self Registration, My Profile, etc.
- Delegation to the business owner to administer and manage sites they own as well as tier 1 service desks
- Link into automated site provisioning process
- Integration to other LOB systems

Azure AD B2B and Office 365



- Azure Active Directory Business to Business
- Allows external users to access Office 365 and any other system exposed through AAD
- Completely free for external users in Office 365
- 1:5 licensing ratio only applies to Azure AD Premium features
- Invite as many external users as you'd like

Invitation Options for Azure AD B2B

Office 365

- **Invite through any of the Office 365 services**
  - SharePoint
  - Teams
  - Outlook Groups

Azure Portal

- **Very technical portal**
- **Can delegate the guest inviter role**
- **Azure Entitlement Manager can be used with AAD P2**

Extranet User Manager

- **Simple delegation and on-boarding**
- **Self-registration**
- **Public and private registration links**

Custom

- **Leverage Graph API**
- **Integrate with Flow, Logic Apps, or Power Apps**

How does Azure AD Premium Licensing fit in?

- **Adds paid capabilities on top of your existing directory**
- **Paid capabilities can be extended to external users accessing your resources through Azure AD B2B**
- **You can invite up to five guest users for each Azure AD license**

Example

- Organization with 500 staff licensed for AAD Premium P2
- Up to 2,500 guest users can also benefit from the AAD Premium P2 features at no additional cost

Azure AD B2B Onboarding Experiences

Existing Office 365

- Logs in with their Azure AD credentials
- Seamless experience
- Single sign-on if already signed into Office 365
- Also works for Microsoft accounts

No Azure AD Account

One time passcode

- Emailed at sign-in
- Valid for 10 minutes
- Low friction, no new account to setup or password to remember
- Validates at each sign in that they still own the email address

Create an account and password

- AAD takes care of password management

Gmail User

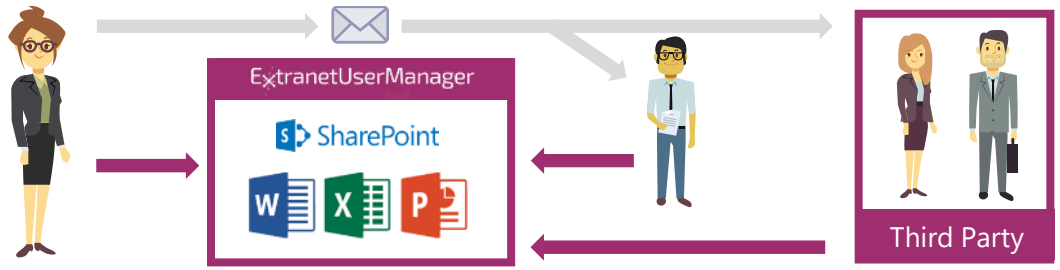
- Federation with Google accounts now also supported
- Same seamless login experience as Office 365
- Must be an @gmail.com address

Why Extranet User Manager with Office 365?

Office 365 and Azure AD B2B Native

- **External Sharing is not scalable**
  - Individual users need permissions management to invite
  - Permissions become a mess, governance goes out the window
- **Azure B2B is not end user friendly**
  - Azure portal is overwhelming
  - All or nothing delegation
- **No self-registration**
- **No integration to other line of business systems**
- **No integration to on premises AD**

- **EUM provides the self-registration, profile management, and delegation**
- **As users and groups are created by the business owners, they are setup in Azure AD by EUM**
- **EUM sends the invitations**
- **Azure AD manages the login process**
- **EUM manages the group membership leveraged for permissions**



Three Structured External Sharing Scenarios

Invitation Only

- Business owner knows who to invite
- Direct one of invitations
- Bulk import of external users

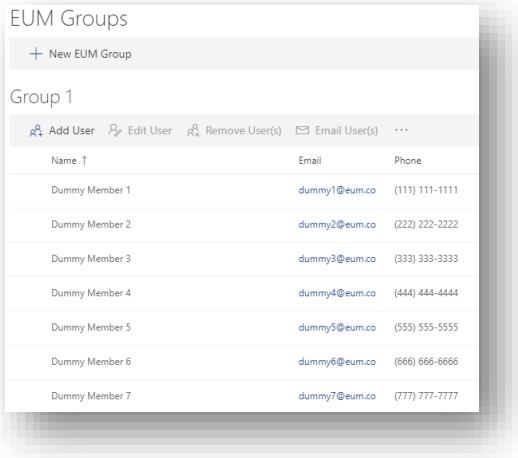
Private Registration

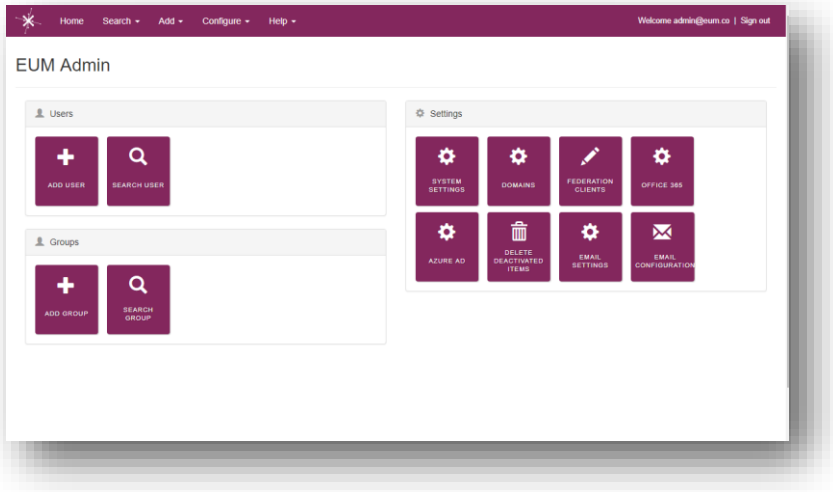
- Business owner knows someone who knows who to invite
- Private registration link that is not easily guessed
- Can be forwarded any number of times
- May or may not want approvals on registration
- May auto-approve based on email domain

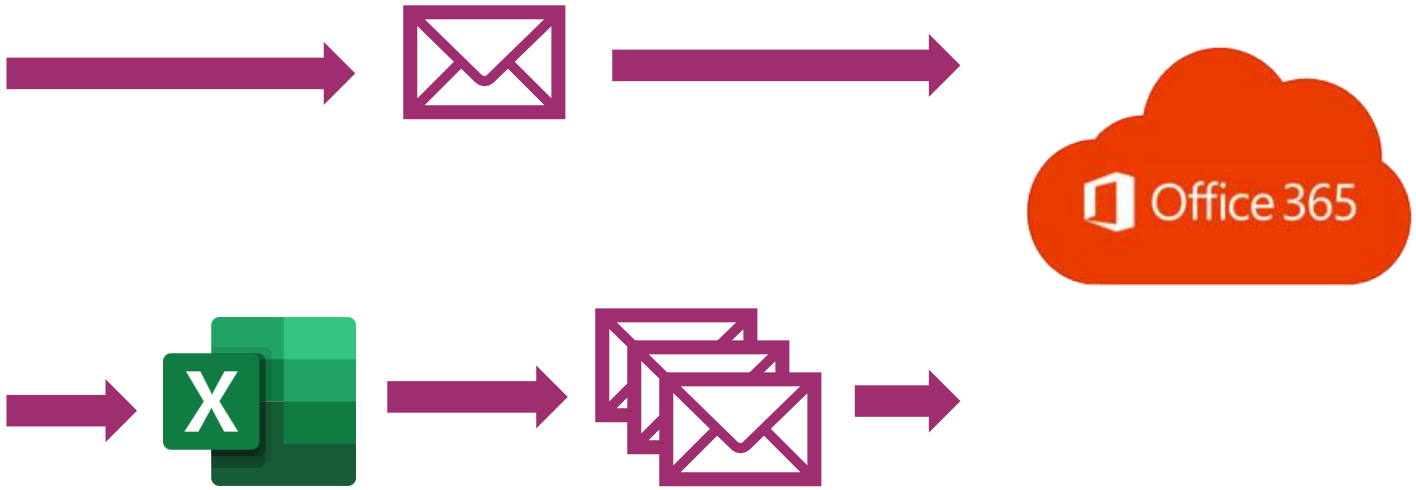
Public Registration

- Anyone should be able to discover and register
- Typically linked from a public website page
- May or may not want approvals on registration
- May auto-approve based on email domain

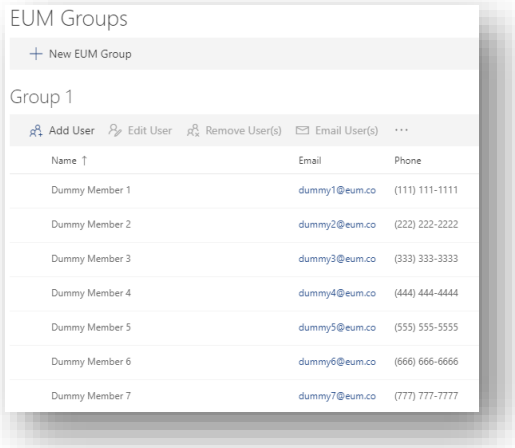
Invitation Only

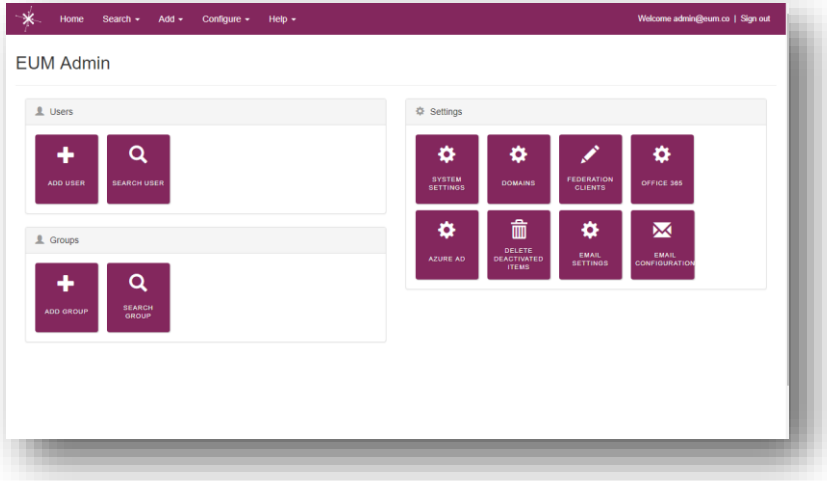


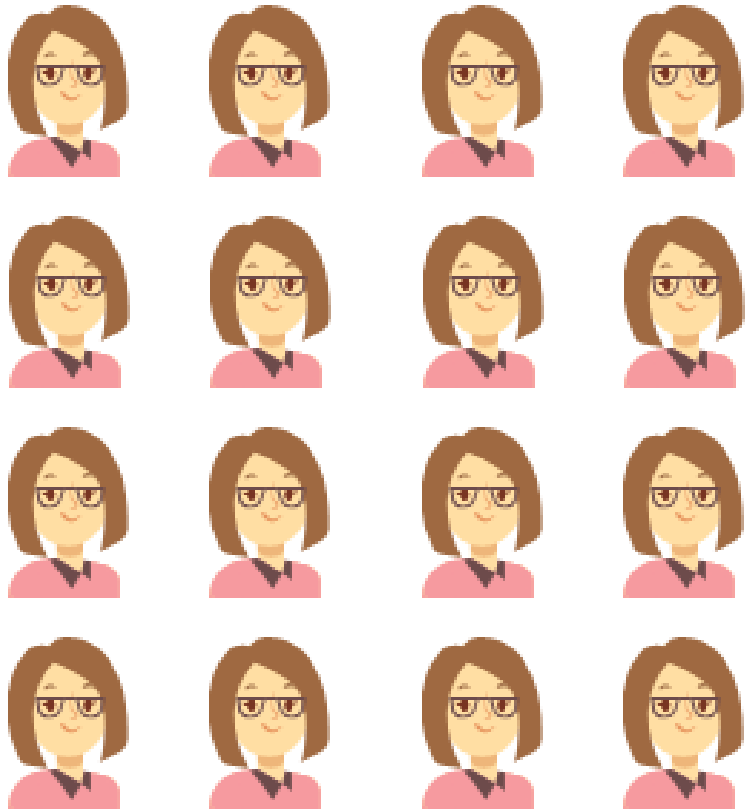




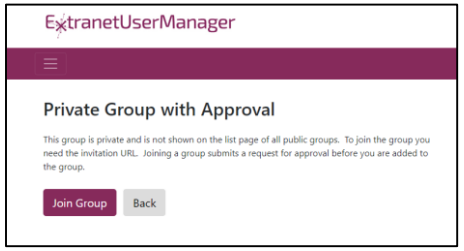
Private Registration

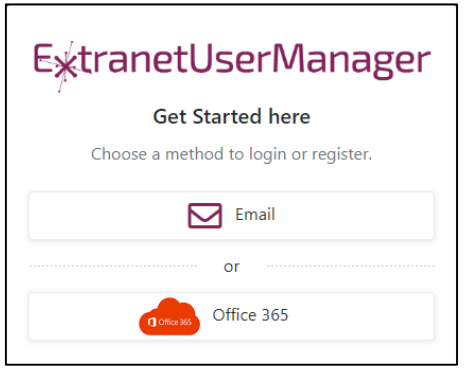


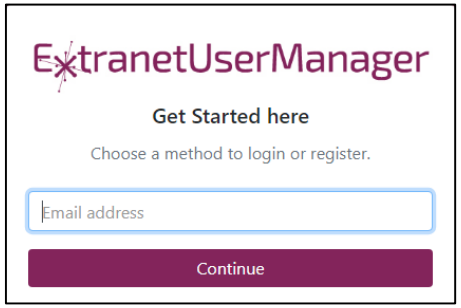


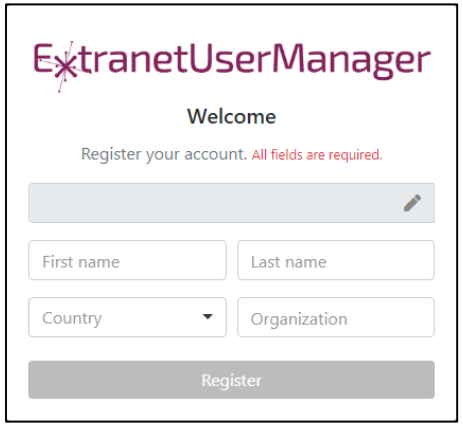


Private Registration

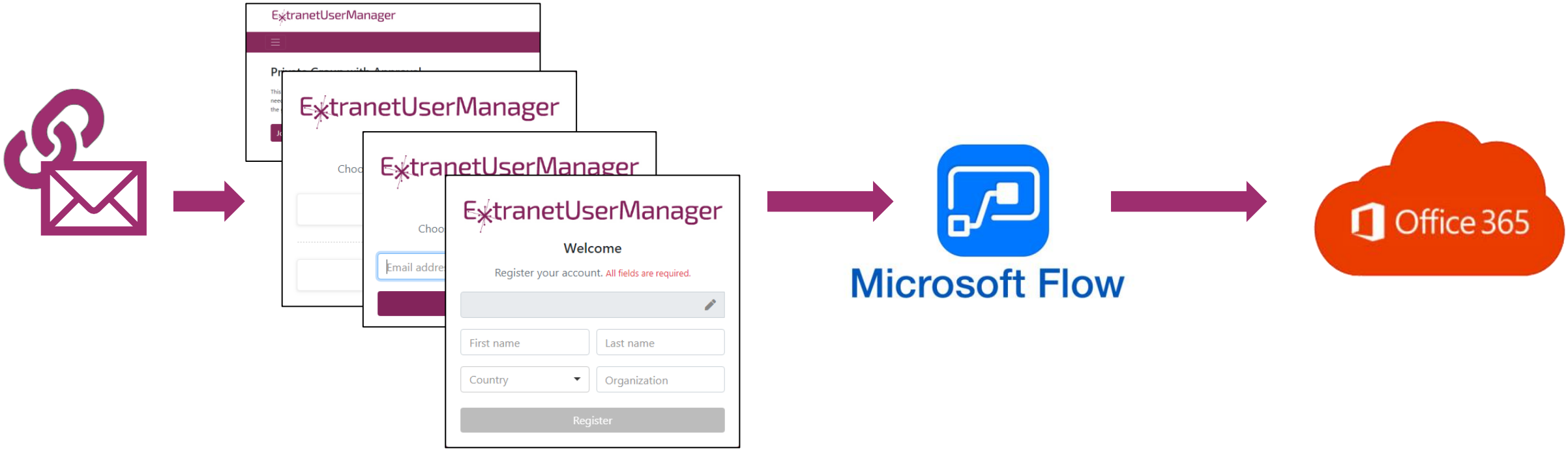




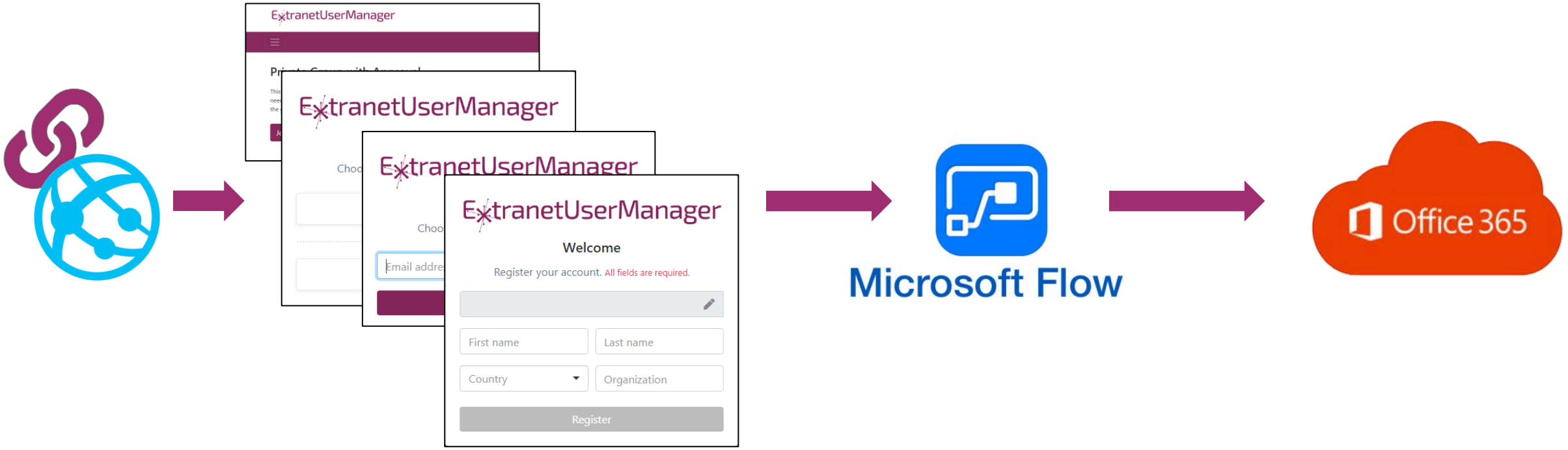




Private Registration



Public Registration



Demo – Office 365

Registration through to Login

Demo Scenario

- **Office 365 sample site at https://eumdemo.sharepoint.com/sites/landing**
  - SharePoint Online in Office 365
- **EUM installed at https://login.eumdemo.com/landing**
- **External users**
  - Setup in Azure B2B
  - Authenticated through Azure AD login form
  - Users managed with the Envision IT Extranet User Manager

Client Spotlight:

Customer Case Study: PhRMA

- PhRMA represents the country's leading biopharmaceutical research companies and supports the search for new treatments and cures.
- PhRMA members invest billions in research and development of new medicines
- Fully migrated to Office 365 internally and utilizes SharePoint Online for collaboration with member organizations
- With over 30,000 potential members, PhRMA partnered with Extranet User Manager to build a scalable, secure extranet in SharePoint Online
- EUM Custom API is utilized for integration into existing LOB systems

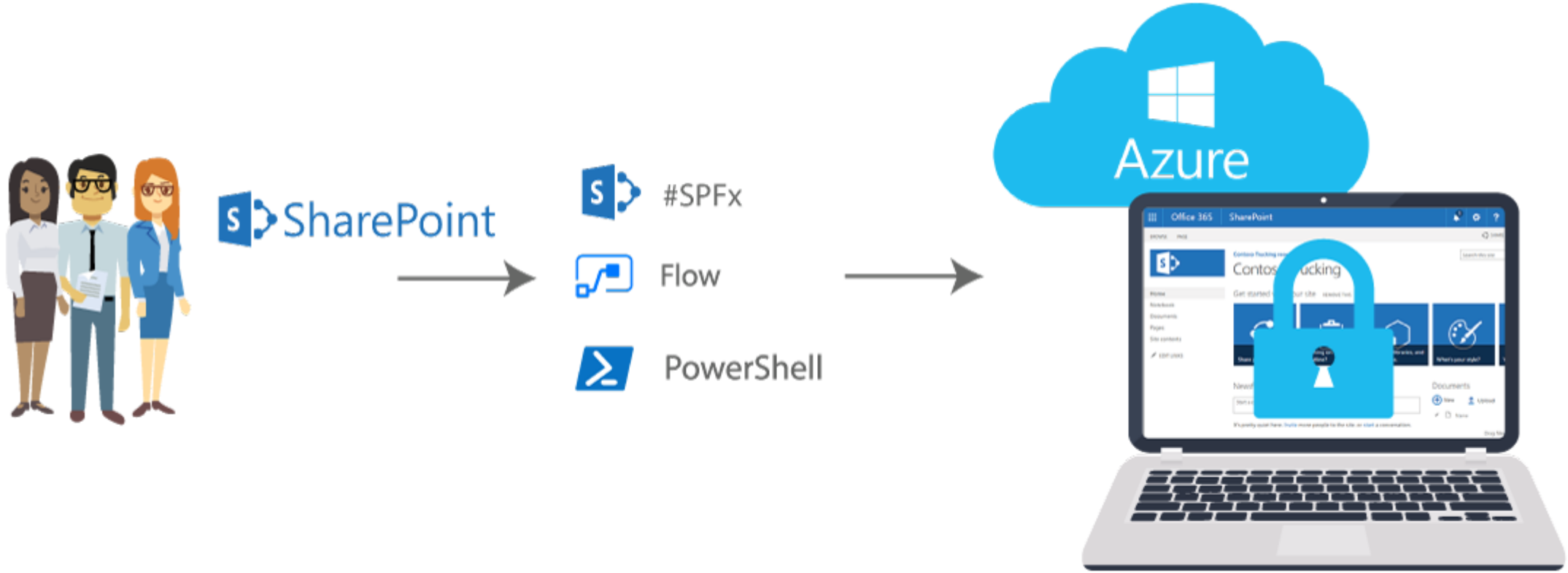
Customer Case Study: PhRMA Office 365

- PhRMA has a robust security strategy for both internal and external users with Office 365
- Leverage Azure Active Directory Premium P1 and P2 functionalities including:
  - Conditional Access Policies steer both internal and external users down separate authentication paths
  - Multi-Factor Authentication is utilized to verify their identity
- Currently have 630 paid Azure AD licenses for all internal users and this more than supports the 1:5 licensing ratio to utilize premium capabilities on Guest users as well
- Have roughly 1500+ users managed by EUM who exist as Guest users in the tenant

Interview Questions for Ryan

- In your project intro you mentioned about 1,500 guest users. Can you describe how that community grew to where it is, and where you see it potentially going from here?
- MFA is a great way to increase the security of your systems, but it can be confusing for end users. Particularly with external users, this can be difficult to manage. Can you describe challenges you had with adoption and how you overcame that?
- One of Extranet User Manager's key features is its extensibility, with a full API and connectors to Power Apps, Power Automate, and Logic Apps. Can you describe how PhRMA leveraged this to integrate EUM into your other systems?

Microsoft Teams, O365 Groups, and Team Site Provisioning White Paper



Project Documentation

- **Source code is available on GitHub at** https://github.com/petercarson/eum-sites/tree/V2
- **Full consolidated whitepaper with step by step instructions** https://www.extranetusermanager.com/resources/articles/site-provisioning-whitepaper-v2

Take a Test Drive for a chance at 1 of 3

$200

Cash Prizes!

Scan the QR Code

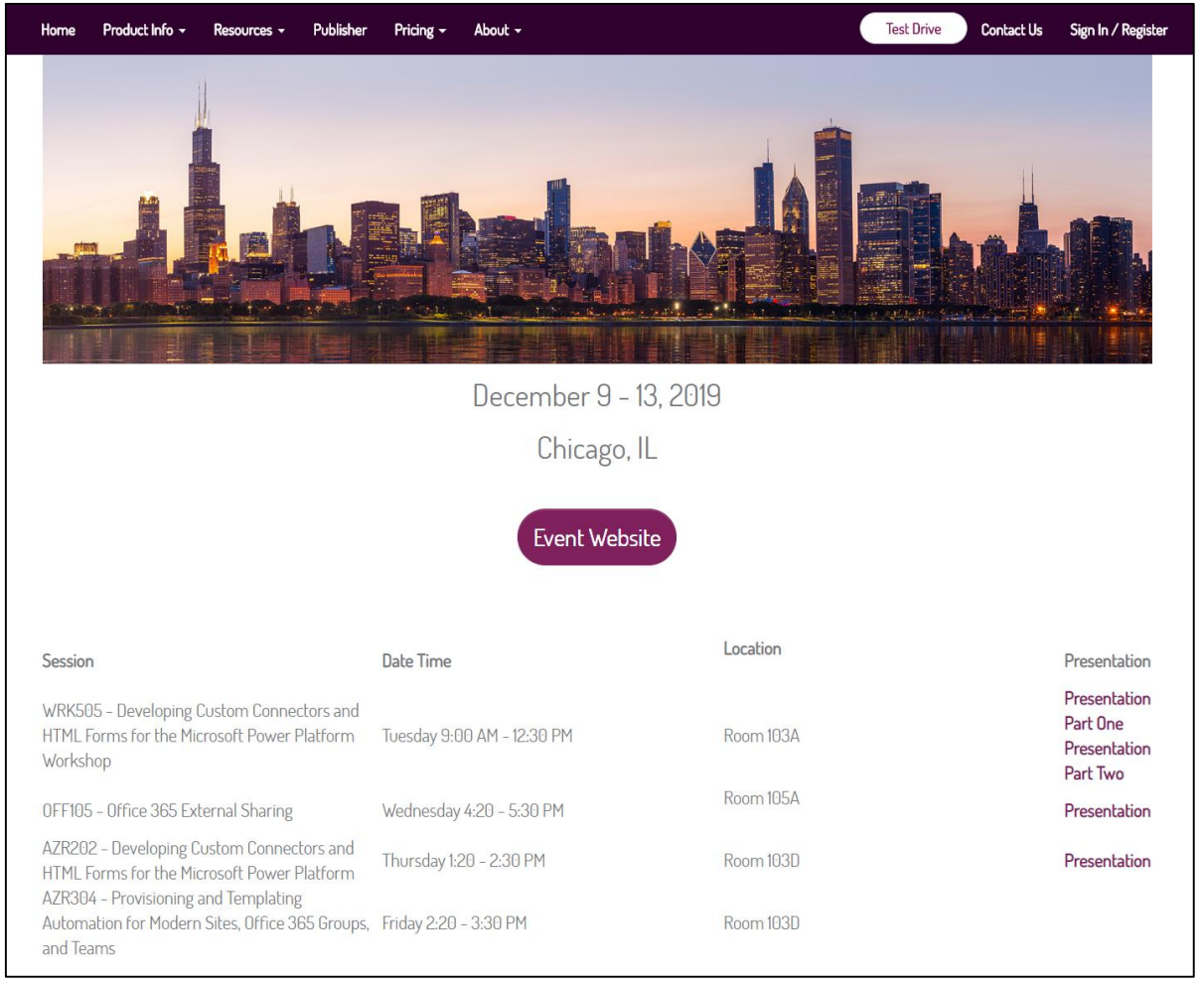
http://eum.co/test-drive

Register and join a group

Access O365

Quick survey to enter Raffle

http://eum.co/resources/events



Thank you!

Questions?