



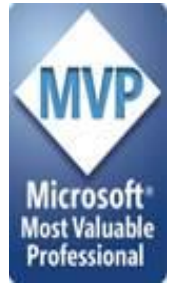
# Enhance the Security of Your Office 365 Extranet

Tuesday, December 3, 2019  
12 - 1 PM EST

# Peter Carson



- President, Extranet User Manager
- Office 365 Apps and Services MVP
- [peter.carson@extranetusermanager.com](mailto:peter.carson@extranetusermanager.com)
- <http://blog.petercarson.ca>
- [www.extranetusermanager.com](http://www.extranetusermanager.com)
- Twitter @carsonpeter
- President Toronto SharePoint User Group



# Logan Guest

## Sales

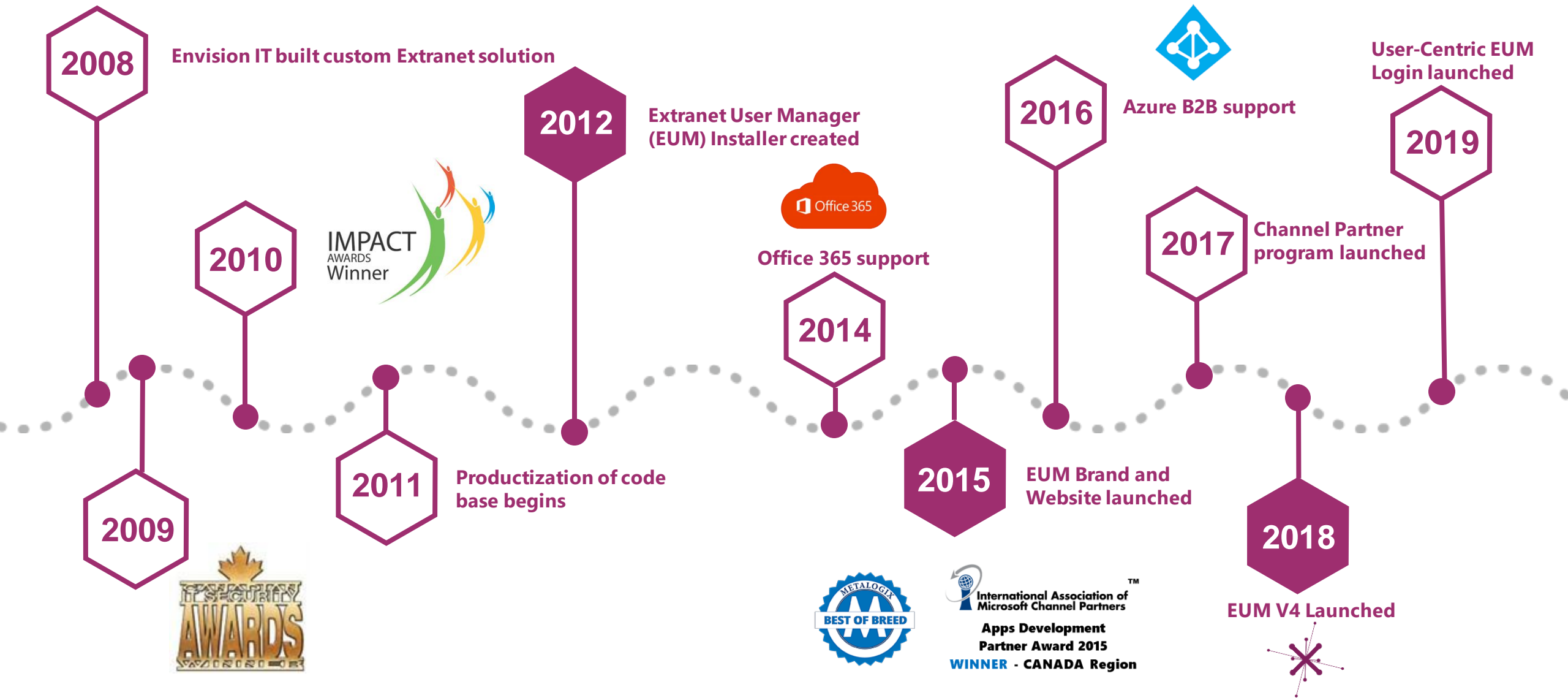
- e: [logan.guest@extranetusermanager.com](mailto:logan.guest@extranetusermanager.com)
- p: (647) 265-8256



# Ryan Hayden

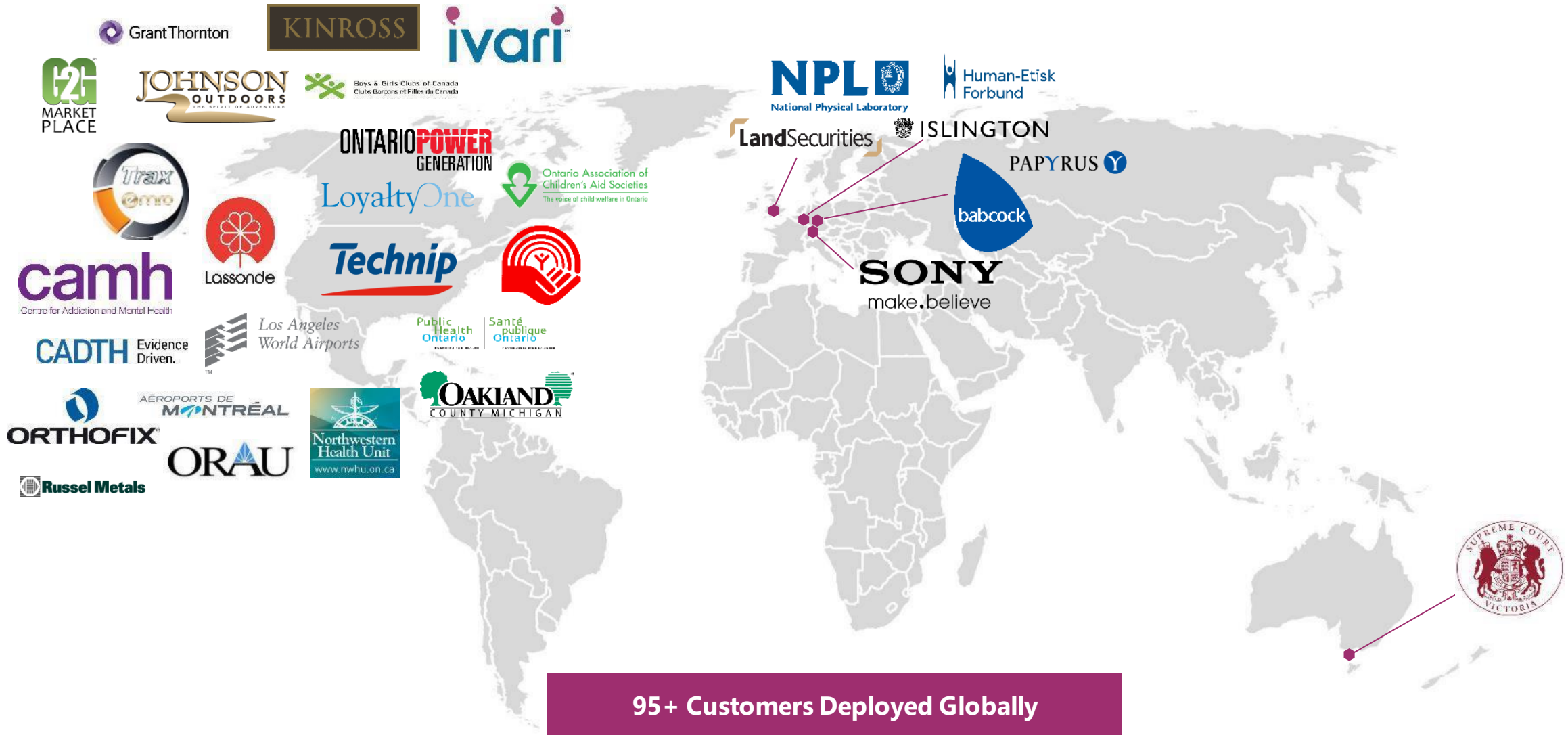


- Enterprise Architect, PhRMA



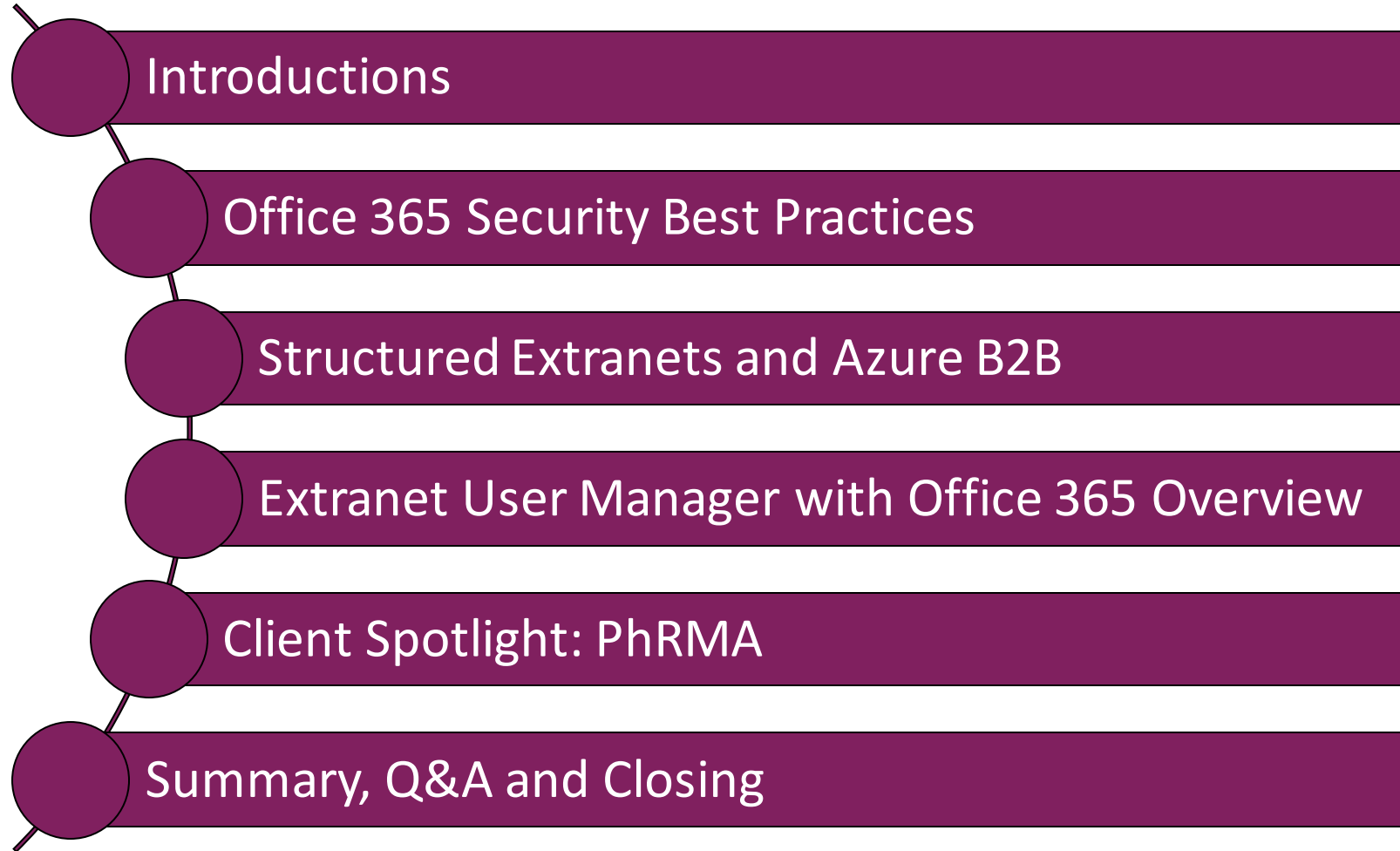


# Customers around the Globe



95+ Customers Deployed Globally

# Agenda



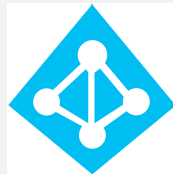
# Poll – Which do you use today?



**Office 365**

**Microsoft 365**

**Enterprise Mobility + Security**



**Azure AD Premium P1 or P2**



# 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>



# 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



# 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

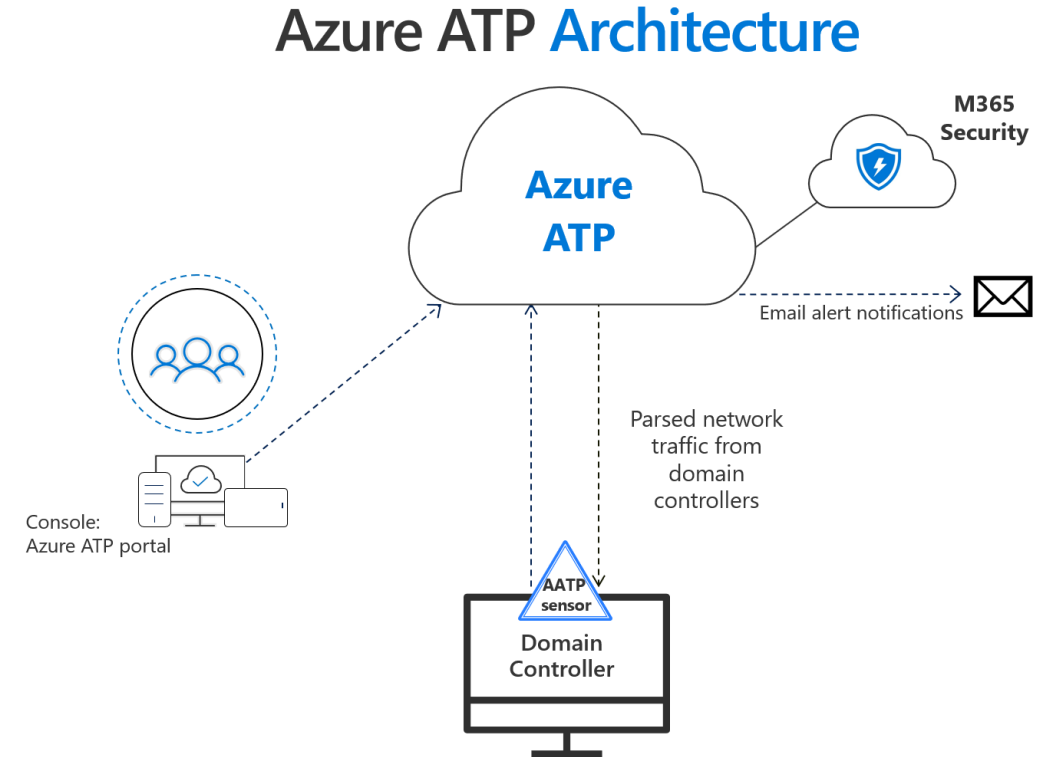
- Multi-factor authentication with Conditional Access
- Hybrid Identities
- Password protection (custom banned passwords)
- Advanced Security and Usage Reports
- Conditional Access based on group, location, and device status
- AIP integration
- And [Much More](#)

## Azure AD Premium P2

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

# Azure Advanced Threat Protection (ATP)

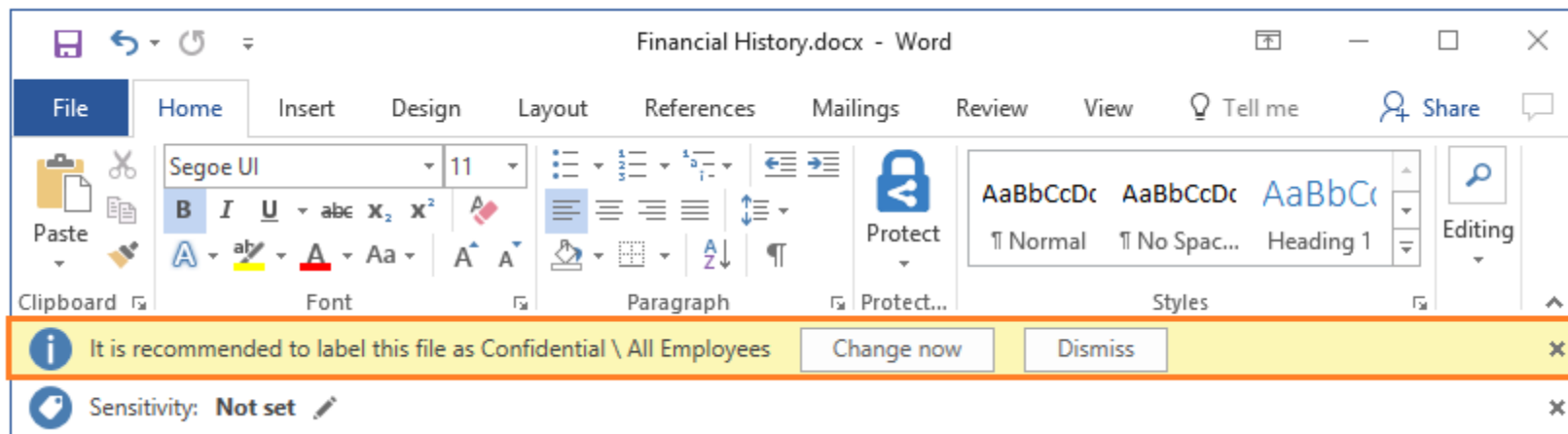
- Cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
- Monitor users, entity behavior, and activities with learning-based analytics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



# 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

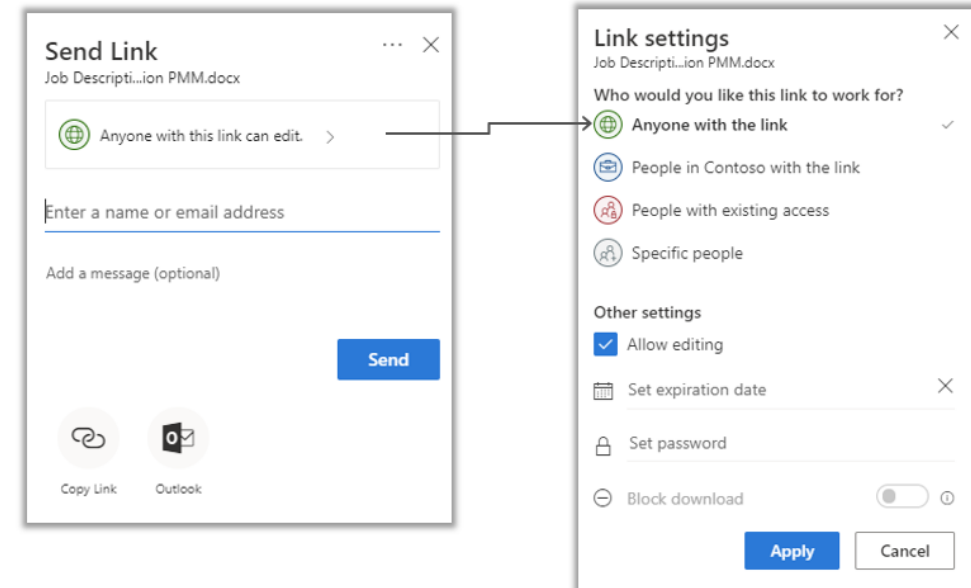
- Granular conditional access at site level with MFA (Multi-factor-authentication)
- Office 365 unified instant access revocation
- Conditional access for Office 365 App Group



# Securing Your Office 365 Extranet

# Unstructured Extranets with Office 365 External Sharing

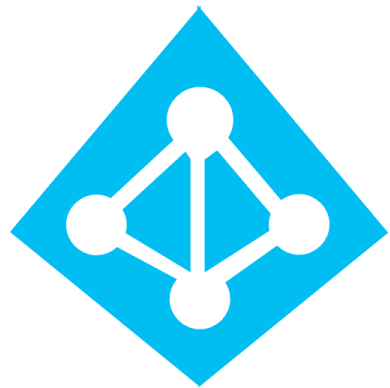
- **External Sharing in Office 365 strongly supports ad-hoc collaboration**
- **Sharing documents with a few to a few dozen external people**
- **Secure Link sharing to sites, libraries, and documents**
  - Anyone with the link (Anonymous)
  - People in your Organization
  - People with existing access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



# 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

# 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

# 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**

# Azure AD B2B MFA Experience

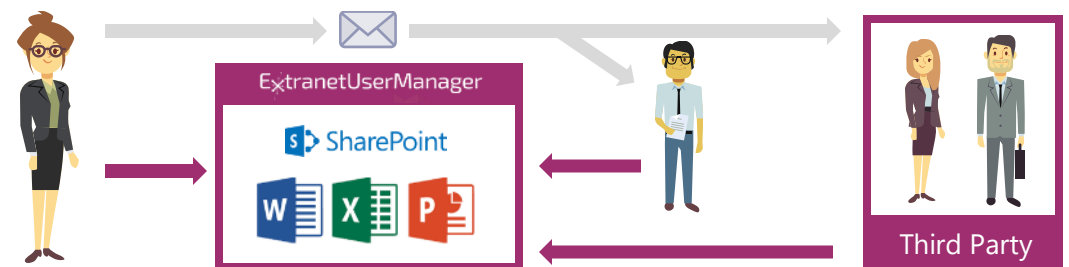
- **Conditional Access Policies** can be used to require MFA for guest users
- **Guests need to register in the Extranet tenant's MFA**
- **They may already have MFA requirements in their own tenant**
- **In some situations they may experience a double MFA**
  - One for their tenant's sign in
  - Again to access the B2B Extranet



# 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**



# 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

# 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

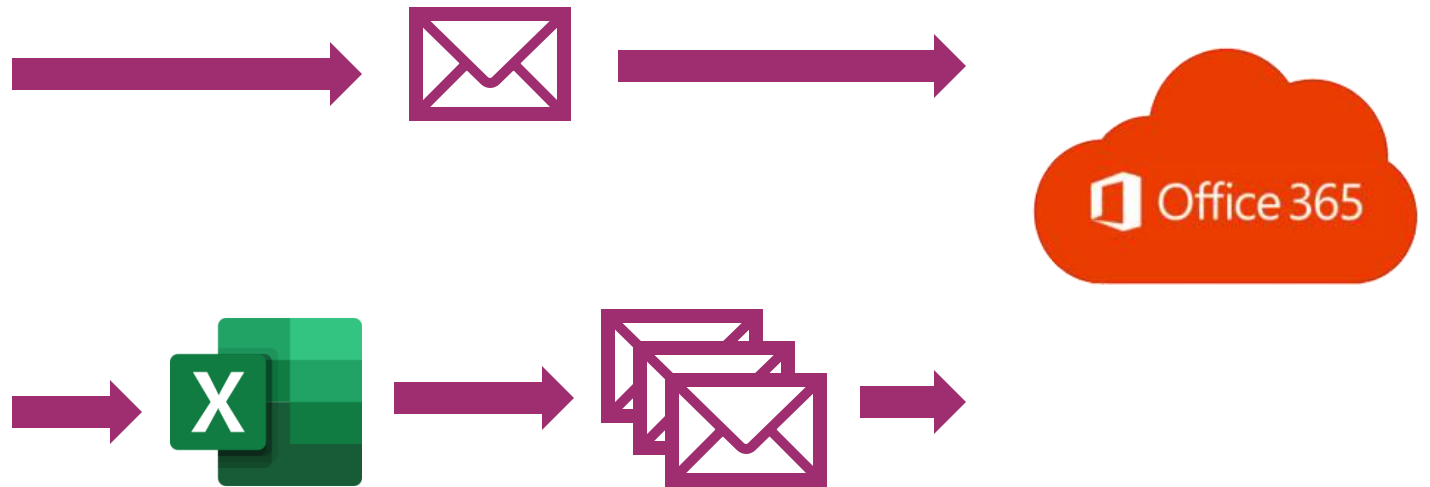
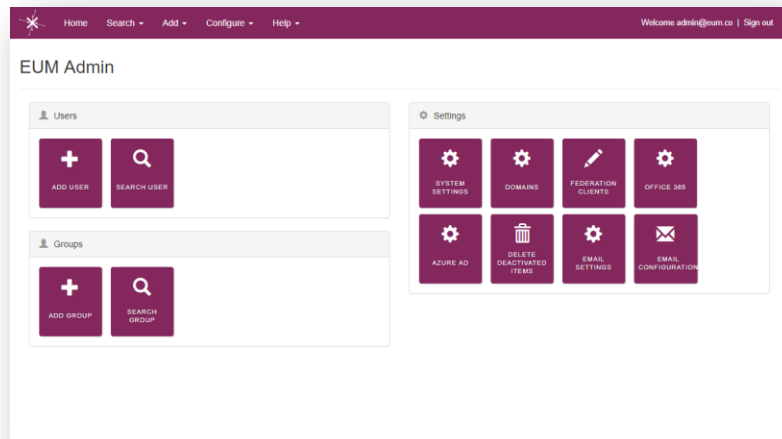
EUM Groups

+ New EUM Group

Group 1

+ Add User - Edit User - Remove User(s) - Email User(s) - ...

Name ↑	Email	Phone
Dummy Member 1	dummy1@eum.co	(111) 111-1111
Dummy Member 2	dummy2@eum.co	(222) 222-2222
Dummy Member 3	dummy3@eum.co	(333) 333-3333
Dummy Member 4	dummy4@eum.co	(444) 444-4444
Dummy Member 5	dummy5@eum.co	(555) 555-5555
Dummy Member 6	dummy6@eum.co	(666) 666-6666
Dummy Member 7	dummy7@eum.co	(777) 777-7777



# Private Registration

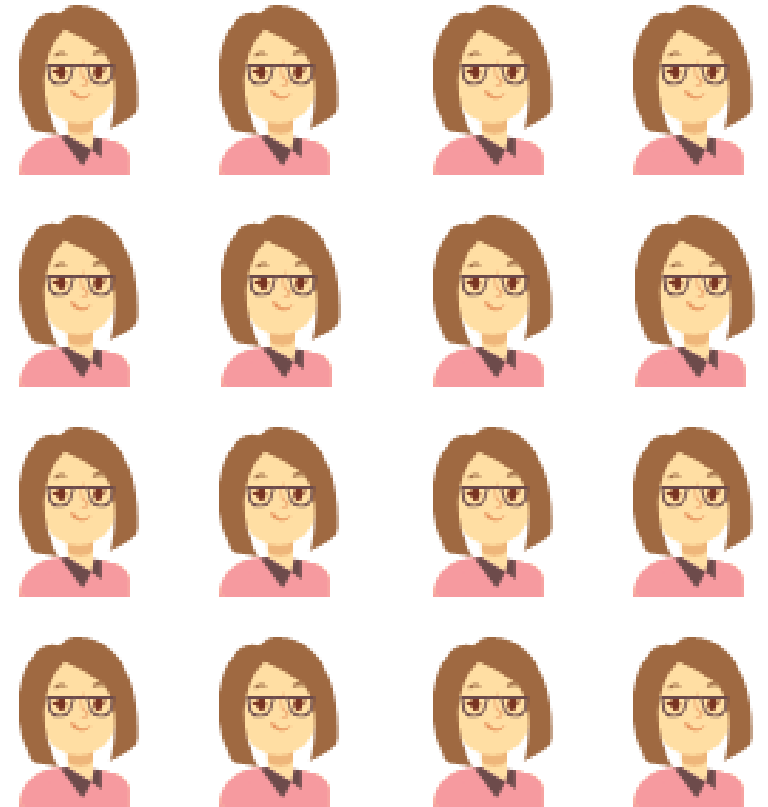
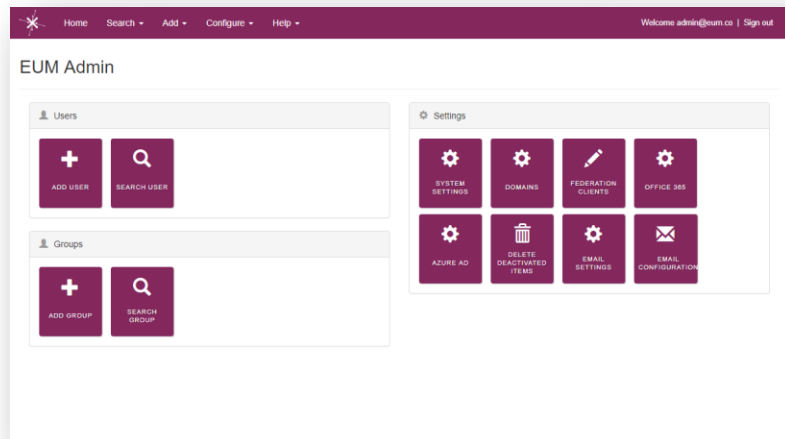
EUM Groups

+ New EUM Group

Group 1

+ Add User - Edit User - Remove User(s) - Email User(s) - ...

Name ↑	Email	Phone
Dummy Member 1	dummy1@eum.co	(111) 111-1111
Dummy Member 2	dummy2@eum.co	(222) 222-2222
Dummy Member 3	dummy3@eum.co	(333) 333-3333
Dummy Member 4	dummy4@eum.co	(444) 444-4444
Dummy Member 5	dummy5@eum.co	(555) 555-5555
Dummy Member 6	dummy6@eum.co	(666) 666-6666
Dummy Member 7	dummy7@eum.co	(777) 777-7777



# Private Registration



ExtranetUserManager

Private Group with Approval

This group is private and is not shown on the list page of all public groups. To join the group you need the invitation URL. Joining a group submits a request for approval before you are added to the group.

Join Group

Back



ExtranetUserManager

Get Started here

Choose a method to login or register.

Email

or

Office 365



ExtranetUserManager

Get Started here

Choose a method to login or register.

Email address

Continue



ExtranetUserManager

Welcome

Register your account. All fields are required.

First name

Last name

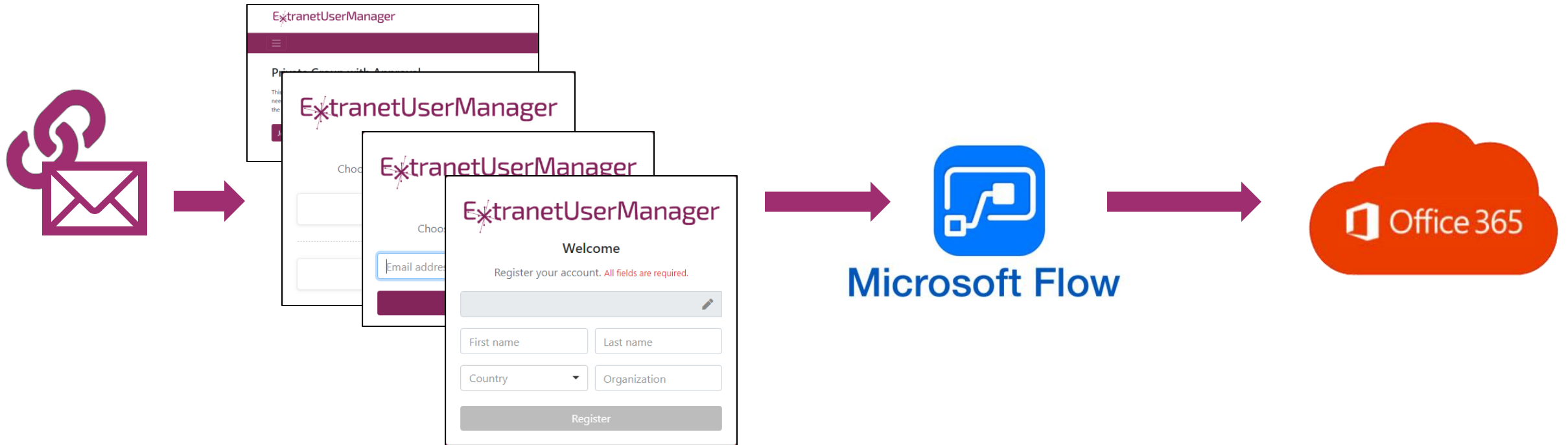
Country

Organization

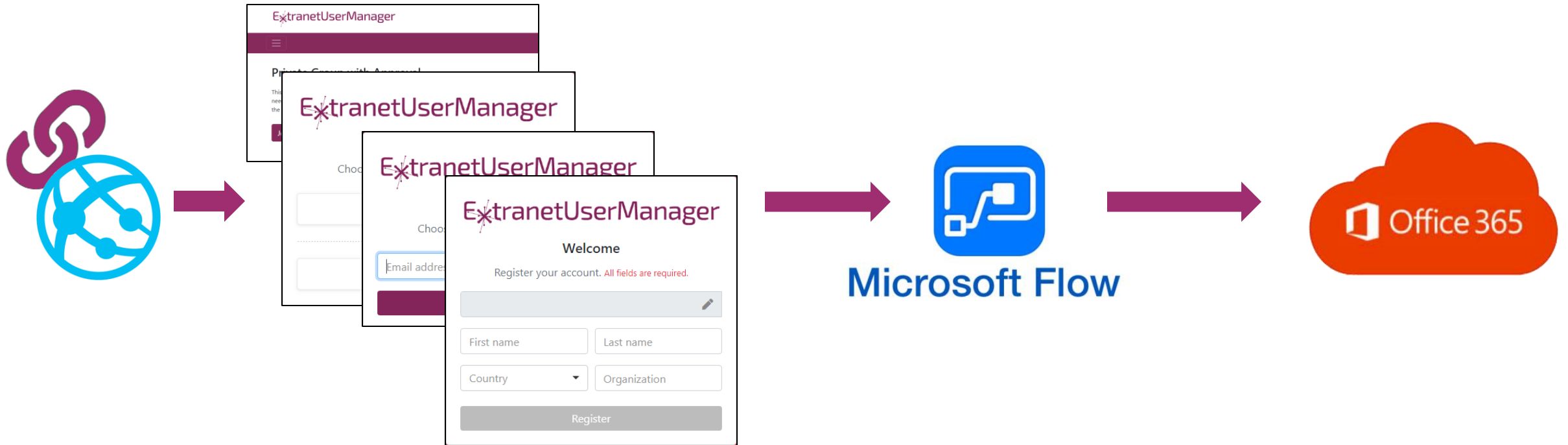
Register



# Private Registration



# Public Registration



# Azure AD P2 Entitlement Management (Preview)

- **Similar to EUM Private and Public Registrations**
- **Supports more sophisticated scenarios through its Access Packages**
  - Assign multiple AAD groups and apps to a user
  - Approval workflows
- **Managed through the Azure Portal**

# Comparing EUM and Entitlement Management

## Extranet User Management

- Streamlined, optimized user experience for guests and business owners
- Simple security structure with a single Azure AD group's membership being managed at a time
- Built in simple workflows can be extended with Power Automate or Logic Apps
- No Azure AD licensing requirement

## Azure AD Entitlement Management

- Complex management through the Azure portal
- Supports complex security scenarios through its Access Packages
- Approval workflow support provided
- Requires Azure AD P2

Each has their place depending on requirements and licensing

# Licensing

# Extranet User Manager Licensing - Monthly

Version	# of Users	Cost	Onboarding (1 Time Fee)
Light Edition	250	\$250 /month	\$800
Standard Edition	250 – 5000	\$400 /month	\$1,600
Enterprise Edition	5000 +	\$650 /month	\$1,600

US Dollars

Full feature set and pricing details available at <https://www.extranetusermanager.com/Pricing>

# Demo – Office 365

Registration through to Login



# Demo Scenario – EUM Testdrive

- **TestDrive:** [eum.co](http://eum.co)
  - Click Test Drive
  - Select the Shortcut Path
- **Office 365 sample site at** <https://eumdemo.sharepoint.com/sites/PublicGroupNoApproval>
  - SharePoint Online in Office 365
- **EUM installed at** <https://login.eumdemo.com/landing>
- **External users**
  - Request to join Public Group – No Approval
  - Self Register through Extranet User Manager and Setup in Azure B2B
  - Authenticated through Azure AD login form
  - Join Group once Authenticated
  - Redirect through to the b2btestdrive site
  - View Site in SharePoint Online including EUM SPFx Webpart
  - Take Survey for a chance to win!



# 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



PhRMA

# 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

The PhRMA logo is displayed in white serif font within a large, dark purple diamond shape. The diamond is part of a larger graphic design that includes images of healthcare professionals. In the top right, a female nurse in blue scrubs smiles. In the bottom right, a male doctor in a white lab coat holds a laptop. The background of the slide is white with purple geometric accents.

PhRMA

# Upcoming Events



SharePoint Fest Chicago  
December 9 – 13, 2019

WRK505 – Developing Custom Connectors and HTML Forms for the Microsoft Power Platform Workshop

OFF105 – Office 365 External Sharing

AZR202 – Developing Custom Connectors and HTML Forms for the Microsoft Power Platform

AZR304 – Provisioning and Templating Automation for Modern Sites, Office 365 Groups and Teams

<https://www.extranetusermanager.com/resources/events/sharepoint-fest-conference-chicago-2019>

# Thank you!

## Questions?

