Teams and Microsoft 365 Sharing – Unstructured & Structured

TechCon 365 Dallas
November 14, 2024

Peter Carson

- President, Envision IT
- 14X Microsoft M365 MVP
- Regular industry speaker
- pcarson@envisionit.com
- blog.petercarson.ca
- envisionit.com
- extranetusermanager.com
- linkedin.com/in/petercarson
- President Toronto SharePoint User Group

3 Key Takeaways

1   Ensure business satisfaction while IT and Compliance enjoy peace of mind

2   Streamline processes for improved productivity for all parties

3   Control your data and branding while leveraging Microsoft's enterprise-grade security in your M365 tenant

envision IT

Agenda

- Introductions
- Unstructured Sharing with Microsoft 365
- Teams Shared Channels
- Entra ID B2B, Purview, and SharePoint Premium
- Reporting
- Summary, Q&A and Closing

envision IT

The Need for Sharing in the Modern Workplace

- **Email Insecurity**
  - **91%** of cyberattacks are initiated through email phishing (source: [Deloitte](#))
- **Shadow IT Risks**
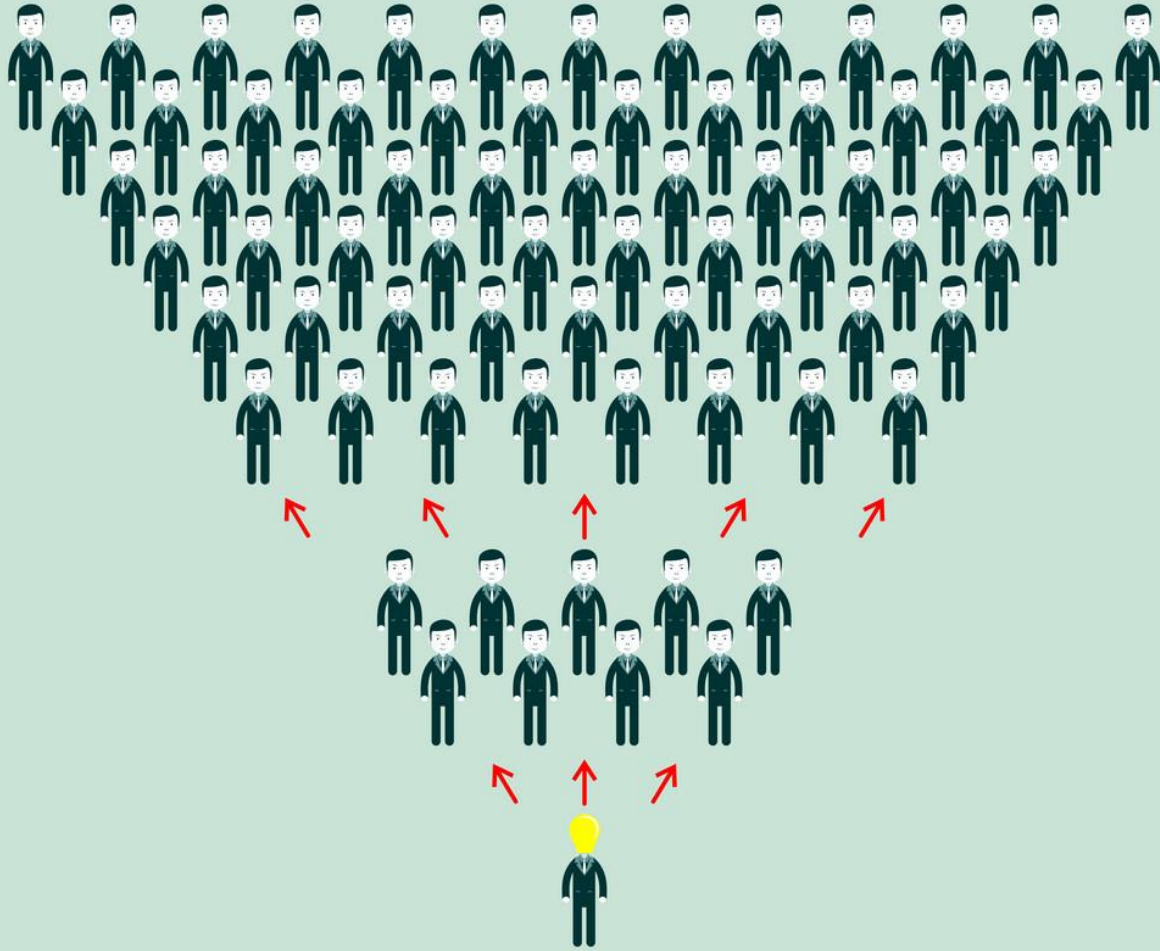- **Widespread Need Across Industries**
- **Centralized Document Exchange**
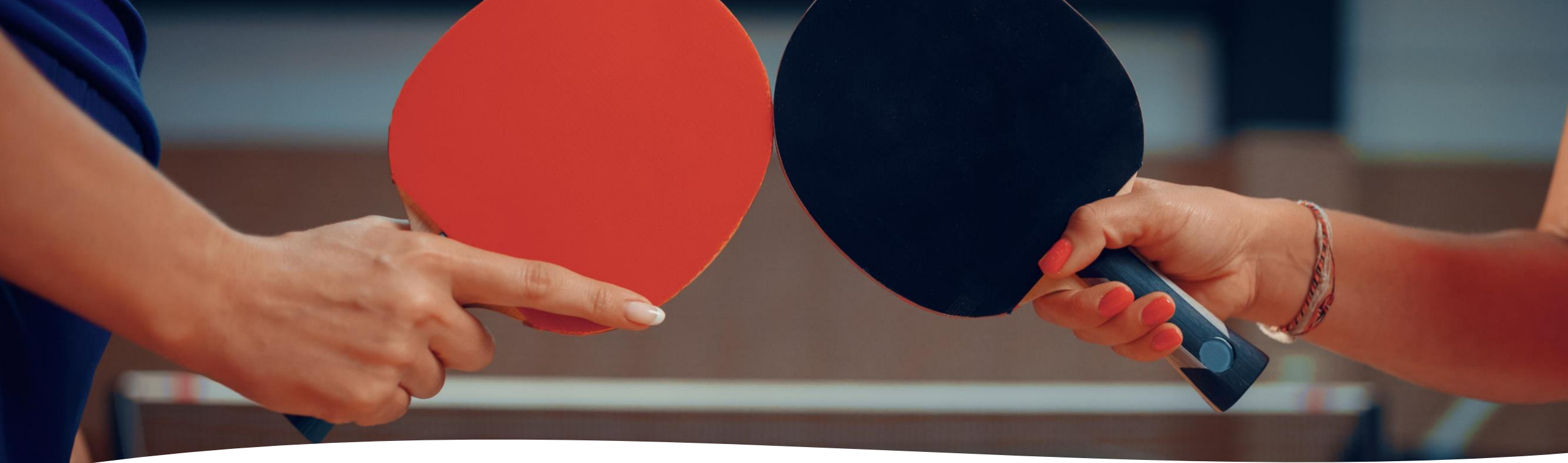
Email Document Exchange: Ping Pong (but less fun)

Using email for document exchange can be a constant back-and-forth, just a game of ping pong.

When Version Control Gets Out of Control

- Email sharing often leads to multiple threads, resulting in multiple document versions
- Without centralized version control, documents can be altered unknowingly
  - Tracking changes becomes nearly impossible
- Each attachment sent multiplies risk of security breach

The Hidden Costs of Insecure Sharing

Data Loss

Financial Drain from Shadow IT

Cyber Attacks

Underutilized Microsoft 365 Investments

Process Management Inefficiencies

# The Choices for 'Under the Radar' Sharing are Endless

envision IT

Why Microsoft 365?

- It's the place your employees are already working
- Users are more likely to use platforms they already understand and trust
- Robust security features, with continuous investment in state-of-the-art cybersecurity measures.
- Extensive compliance certifications

What is Unstructured Sharing in Microsoft 365?

- External Sharing in Microsoft 365 strongly supports ad-hoc collaboration

- Unstructured sharing involves sharing documents with a few to a few dozen external people

- Secure Link sharing to sites, libraries, and documents
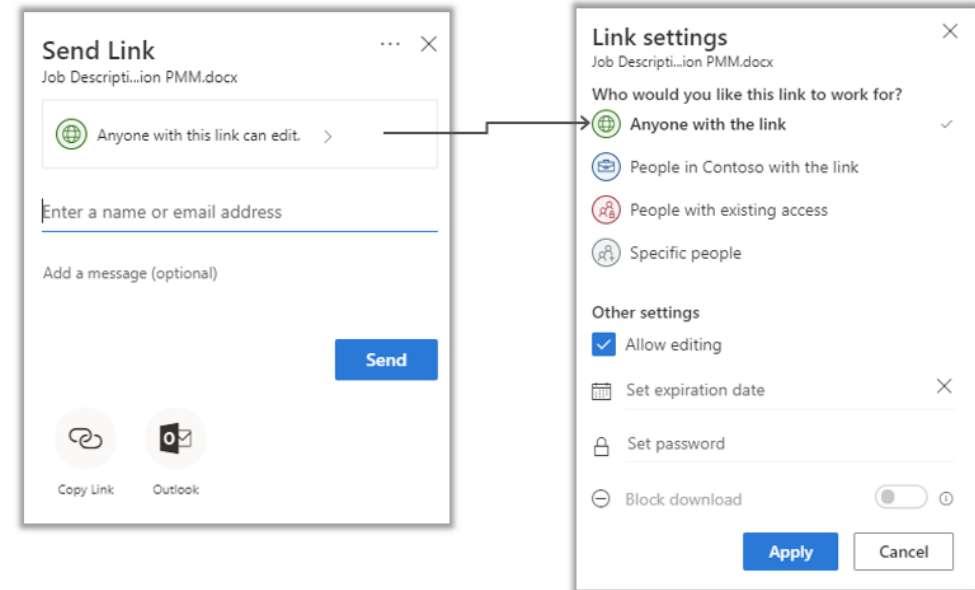
Microsoft 365 Tools for Unstructured Sharing

Request Files with OneDrive for Business

- Ask colleagues and external users to upload files to a folder

- Uploaders can only see their own content

Shareable Links in SharePoint Online

- Enable edit and/or read access to colleagues or external users

- Can modify granularity of access

Teams Guests

- Invite guests into your Team to communicate and collaborate

Teams Shared Channels

- Connect users from a trusted organization to join your channel as if it is in their own tenant

envision IT

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
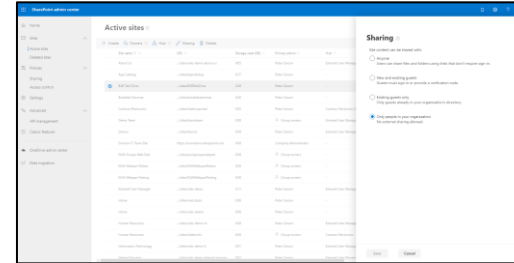- Block externally-shareable edit links
- Disabled

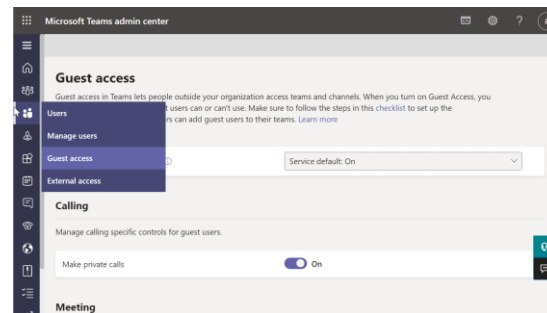# Multiple Places to Configure External Sharing
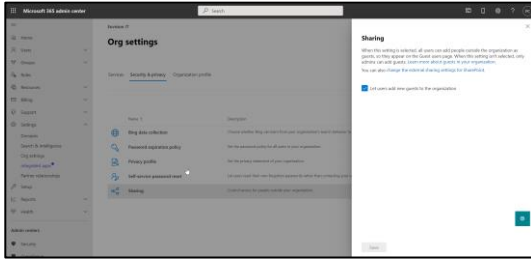
SharePoint Admin

Site Collection Admin

PowerShell

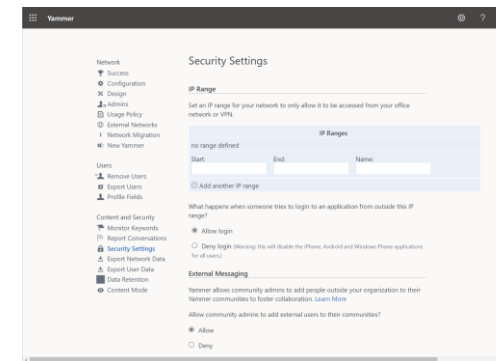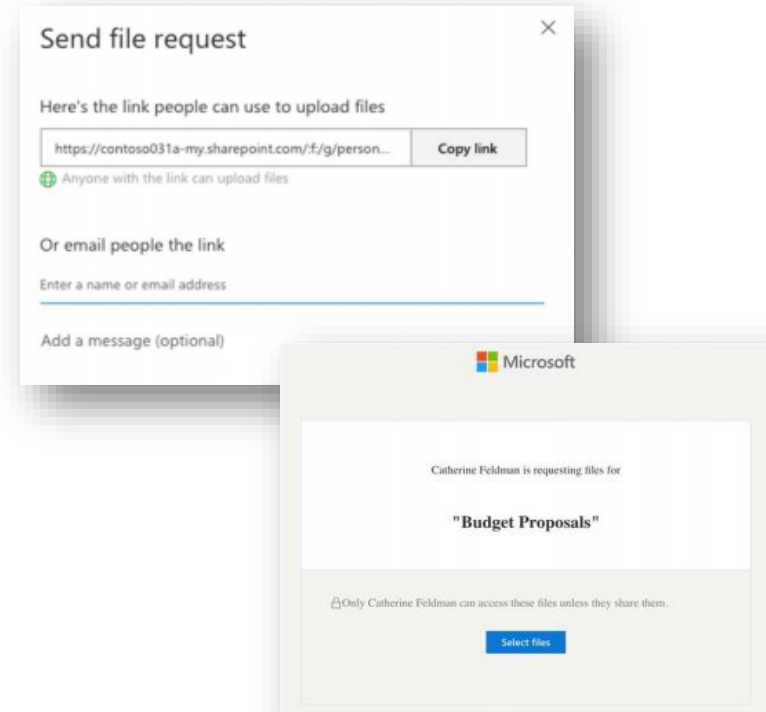Microsoft 365 Admin

Teams Admin

Yammer Admin

envision IT

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

- Branding of request pages announced in the Microsoft roadmap

Enable File Requests in SharePoint or OneDrive - SharePoint in Microsoft 365 | Microsoft Learn

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

B2B Direct 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](#)

Types of Teams Channels

	Standard Channel	Private Channel	Shared Channel
Members	Sames as Team	Subset of the Team members	Any members of the tenant or B2B Direct Connect
Teams	Open to all Team members	Visible only to channel members	
SharePoint	Folder in Team Site collection Documents library All team members have access	New site collection specific to the channel and secured to channel members	
Sharing	B2B Guests	B2B Guests	B2B Direct Connect

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
- Outbound connections don't have to be setup for internal **Shared Channels**

Team

Shared Channel

Team

Team

Private Channel
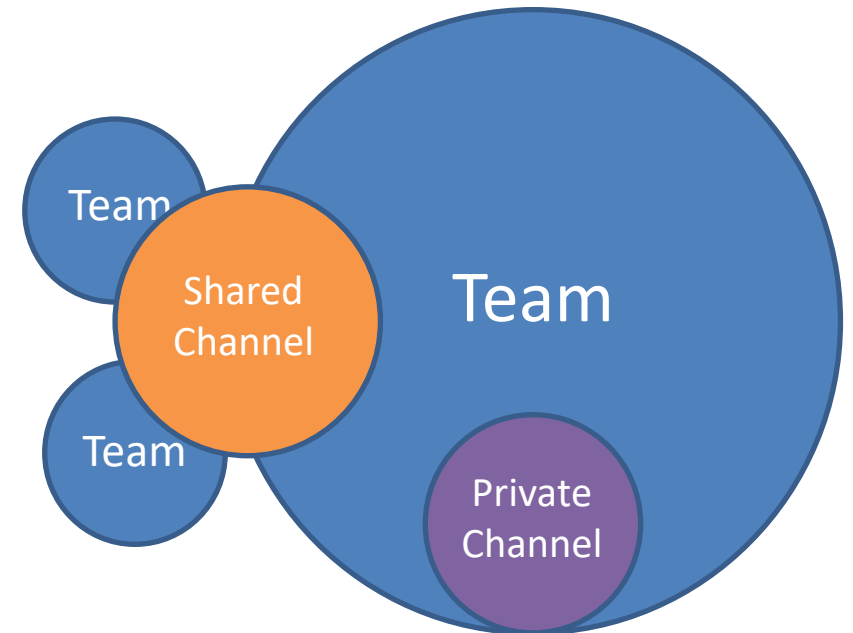
Teams Architecture
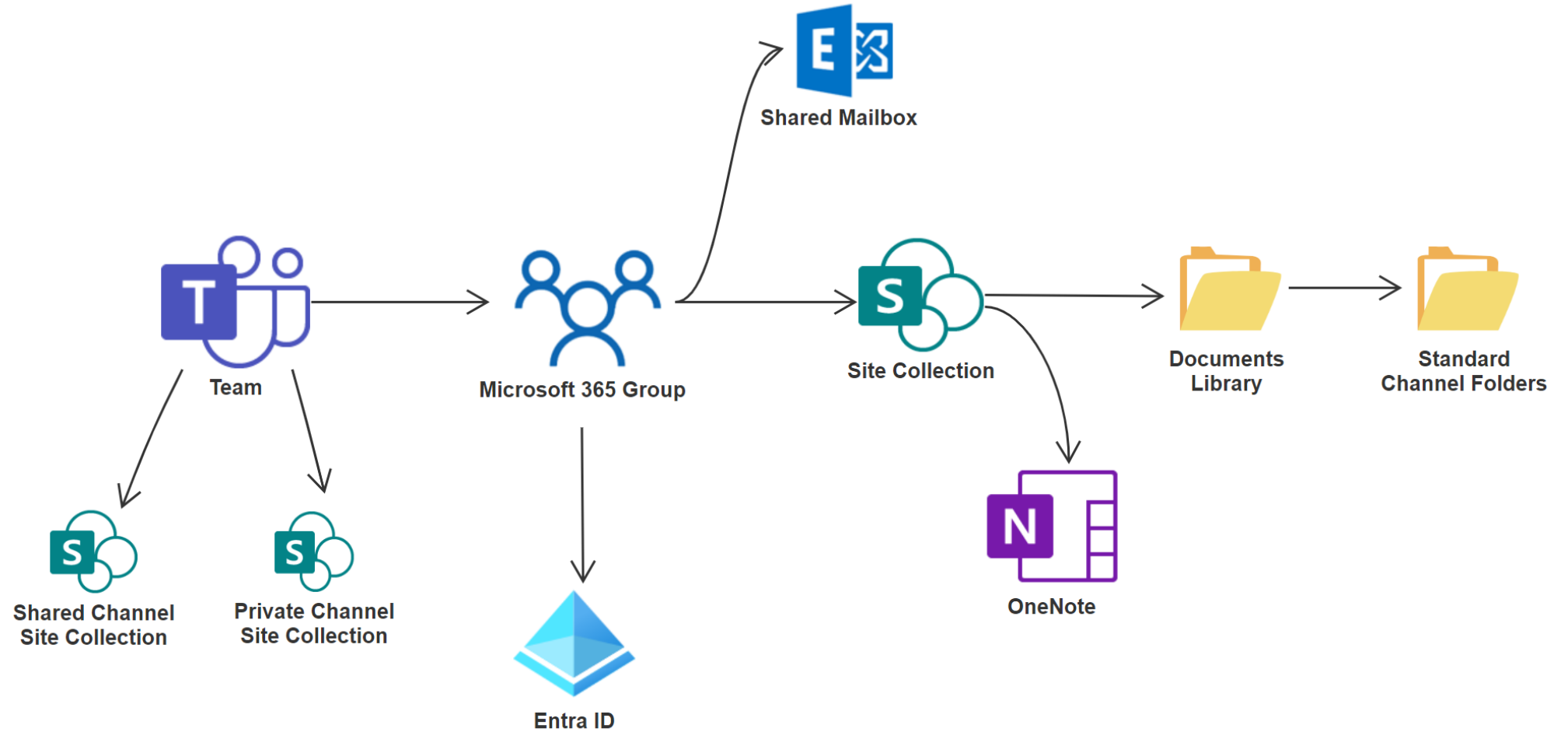
Shared Channel Recap

Great for both internal only and externally shared channels

You cannot share files from the Shared Channel site collection with anyone not in the channel

Do you like the convenience for the external users not having to tenant switch in Teams?

Will 100% of the people you want to invite in belong to an organization your organization can setup B2B Direct Connect with?

Entra ID and Microsoft 365 Licensing

- First 50,000 Monthly Active Users are free for all Entra ID Premium features
  - Minimal costs beyond this
- No licenses needed for guests to access Teams, SharePoint Online, and Viva Engage
- Power BI and Power Apps do have guest licensing requirements
- Microsoft 365 Guests do need to be external
  - Can't consider your front line or unlicensed staff to be guests
  - This is what the Microsoft 365 Front-Line Worker F1 and F3 license is for

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/

Onboarding External Users through Entra B2B

Microsoft 365 User

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

Social User (Google, Meta)

- Federation with Google and Meta accounts now also supported
- Same seamless login experience as Microsoft 365
- Need to be an @gmail.com address for Google Federation

Non-Microsoft 365 Account

- One time passcode
- Emailed at sign-in
- Valid for 30 minutes
- Low friction, no new account to setup or password to remember
- Validates at each sign in that they still own the email address

Email One-Time Passcode Authentication

- Authenticate Guest users without:
  - Azure AD account
  - Microsoft account
  - Social provider - Google or Facebook
- One-time passcode is sent to email address
- Passcode is entered to sign in
- One-time passcode is valid for 30 minutes
- Next user session will send a new passcode to the user

MFA Scenarios

Admins	Guests	Members

• Require MFA on every authentication	• 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
	• Consider trusting partner tenants for MFA
		• 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

Entra ID P1 vs P2

Entra ID Premium 1

- 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
- Azure Information Protection integration
- And [Much More](#)

Entra ID Premium 2

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

Entra B2B Portal 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

Traffic Light Protocol: Simplifying Sensitivity Labels in Microsoft 365

The **Traffic Light Protocol (TLP)** is a classification system that uses color-coded labels to categorize and control the sharing of sensitive information.

- Developed by the UK's National Infrastructure Security Coordination Centre in the early 2000s
- Encourages sharing of sensitive information
- Adopted by the US Cybersecurity and Infrastructure Security Agency (CISA)

TLP Labels and their Meanings
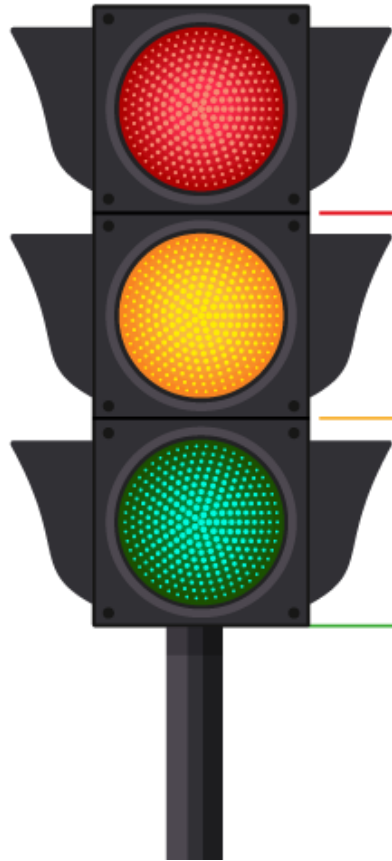
TLP: Red+Strict
Not for disclosure, restricted to participants only.

TLP: Red
Not for disclosure, restricted to participants and clients only.

TLP: Amber+Strict
Limited disclosure, restricted to participants organization.

TLP: Amber
Limited disclosure, restricted to participants organization and clients.

TLP: Green
Limited disclosure, restricted to the community.

TLP: Clear
Disclosure is not limited.

- **Red:** Most sensitive information; requires MFA and document encryption
- **Amber:** Sensitive information; external sharing allowed with MFA
- **Green:** Less sensitive; accessible to guests without MFA
- **Clear:** Public information; accessible without restrictions

TLP and External Access in Microsoft 365

Below is a suggested implementation of TLP for defining guest access in Microsoft 365:

TLP	External Access	Guests Require MFA	Document Encryption	M365 Member Licensing
Red+Strict	No	N/A	Yes	E5
Red	Yes	Yes	Yes	E5
Amber+Strict	No	N/A	No	E3
Amber	Yes	Yes	No	E3
Green	Yes	No	No	E3
Clear	Yes	No	No	N/A

Entra 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

Microsoft Reporting

- [Data access governance reports for SharePoint sites - SharePoint in Microsoft 365 | Microsoft Learn](#)
- Sharing links reports
  - "Anyone" links
  - "People in the organization" links
  - "Specific people" links shared externally
- Sensitivity labels applied to files

Third Party Tools

Envision IT M365 Tenant Dashboard

Workspaces
23-Oct-24

Go to drill-through Reset filters

184 Teams

212 Team sites

43 Communication sites

Workspace Status

< 90 days 83
< 1 year 87
> 1 year 269

Retention Compliance

100%
50%
0%
100.00%

Sensitivity

None
437

Allowed Sharing

None — 0
Existing Guests — 13
Anyone — 15
New and Existin... — 375

Sharing Links

OrganizationEdit — 626
Flexible — 446
AnonymousEdit — 71
AnonymousView — 57
OrganizationVi... — 7

117,311 Count of Files

777.57 File Size (GB)

753 Active storage used (GB)

387 Inactive storage used (GB)

M365 Tenant Dashboard | Envision IT

4 Key Takeaways

1 External sharing happens with or without IT support

2 Microsoft 365 is far more secure than email or shadow IT

3 There are plenty of configuration options

4 Putting the right controls in place is a balance

envision IT

Additional Resources

[EUM Data Room: Confidential Document Exchange Made Simple, Efficient and Secure with Microsoft 365](#)

[Mastering Secure External Sharing in Microsoft 365: A Comprehensive Guide for Structured & Unstructured Sharing](#)

Thank you!

Any Questions?