We'll get you there.

Microsoft 365 Security: Is Your Organization's Data Safe?

October 13, 2022

CPAs | CONSULTANTS | WEALTH ADVISORS

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Introductions

Dave Hale

Director

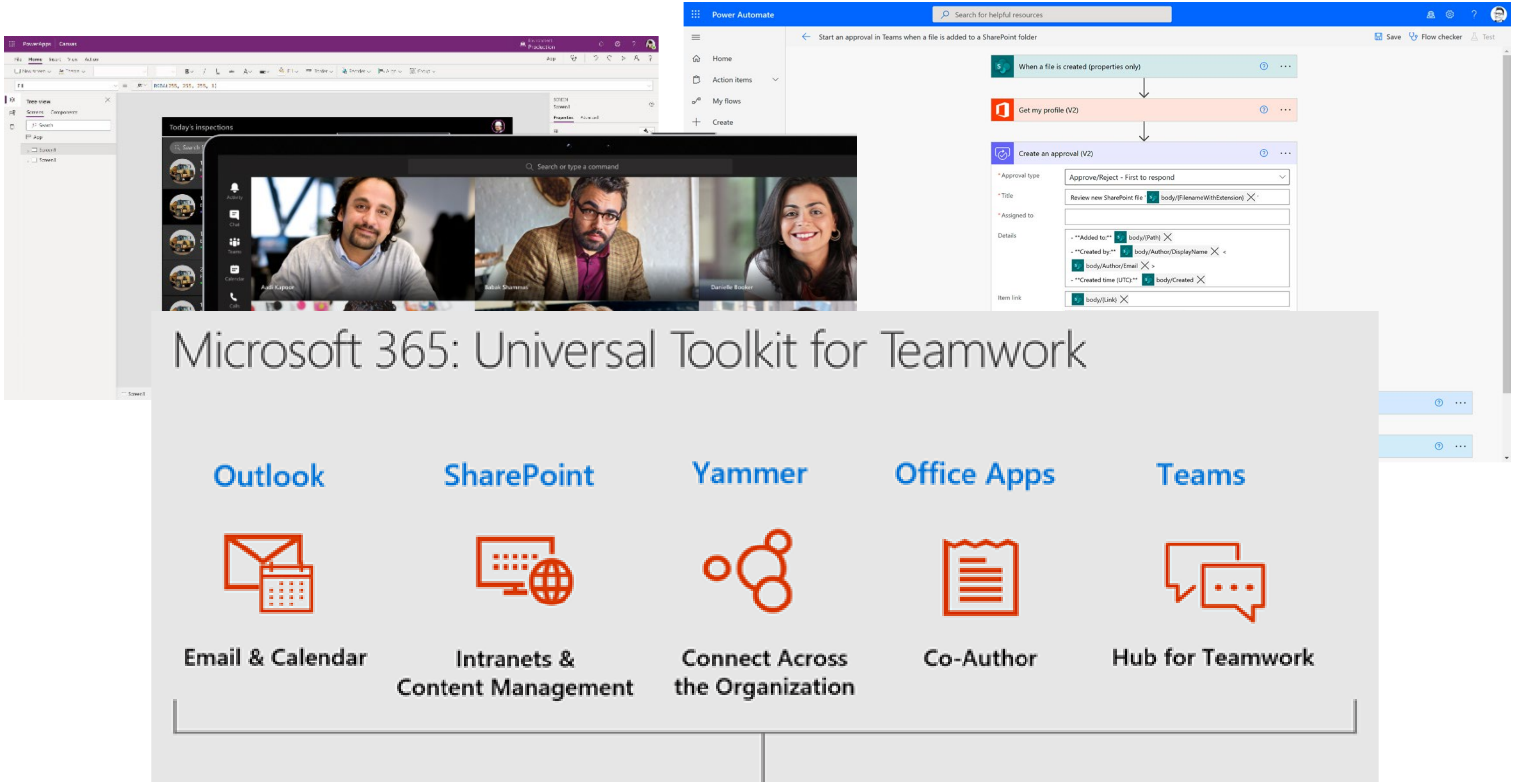
David Sun

Principal

Nehemiah Jones

Cybersecurity Senior

Overview



Start an approval in Teams when a file is added to a SharePoint folder

When a file is created (properties only)

Get my profile (V2)

Create an approval (V2)

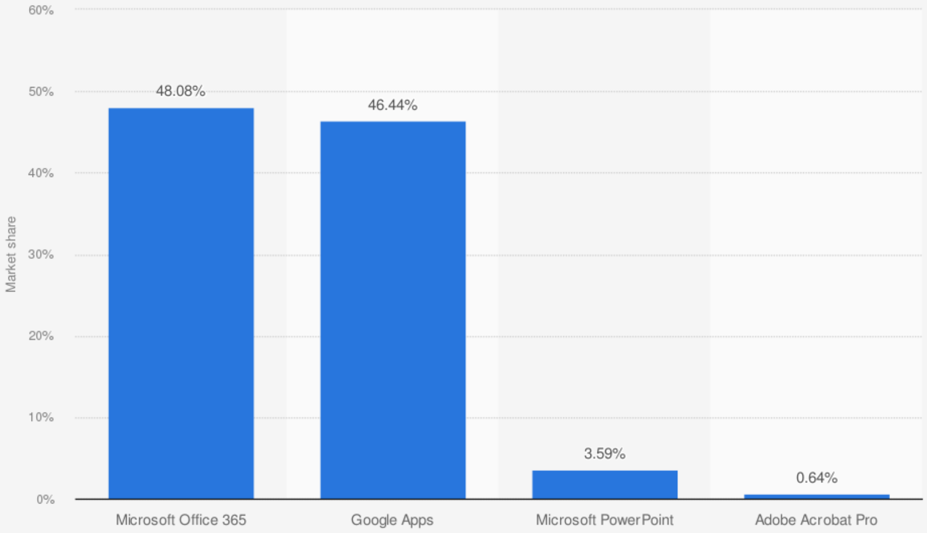
- *Approval type: Approve/Reject - First to respond
- *Title: Review new SharePoint file ' body/{FilenameWithExtension} '
- *Assigned to:
- Details: - **Added to:** body/{Path} - **Created by:** body/Author/DisplayName < body/Author/Email > - **Created time (UTC):** body/Created
- Item link: body/{Link}

Microsoft 365: Universal Toolkit for Teamwork

Outlook	SharePoint	Yammer	Office Apps	Teams
Email & Calendar	Intranets & Content Management	Connect Across the Organization	Co-Author	Hub for Teamwork

Overview

Market share of major office productivity software worldwide as of February 2022



Source
Enlyft
© Statista 2022

Additional Information:
Worldwide; 2016 to 2021*

Overview

- It’s also one of the most compromised cloud platform
- M365 has a rich set of security features (120+)
  - Many are disabled by default
  - Or in the case of Legacy Authentication, it was enabled by default...
  - Most IT admins are familiar with ~15 controls

Typical Migration

- IT implements basic security controls
  - MFA, Conditional Access, Spam filter
  - Time to research and learn new controls?
- As deadlines approach IT is in a rush
  - Ensure data is accurate and complete
  - Make user transition easy as possible
- Uncommon for full security review to be performed prior to migration
- Later- No one wants to break something!

When it all goes wrong

- In responding to numerous BEC/wire fraud incidents, we have seen common themes and issues
- Credentials are obtained
- Log in via Outlook Web (no MFA implemented) or POP3 client (legacy auth) from strange IP address (no Geofencing)
  - Lately attackers have even spammed MFA prompts until a user relents
- Email forwarding rules are created
  - Messages redirected to unmonitored folders (RSS Feeds)
- Hundred$ of thousand$, sometimes million$ lost…

How could this happen?

- The Licensing Maze
  - Insufficient licensing kept the company from using security features (i.e. no advanced email/link filtering)
- Dangers of the Default Config
  - Default configurations were not adjusted since “we should trust Microsoft’s standard config”
- IT Overload
  - IT admins adjusted the config in the past but failed to keep up with new features & threats
- None of the Above
  - There is always a residual risk of cyber threats!

Reason 1: The Licensing Maze

We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Microsoft integrated security

Simplify and fortify security with Microsoft Security solutions

Identity and access management	Threat protection	Information protection	Security management
Protect users' identities and control access to valuable resources based on user risk level	Protect against advanced threats and recover quickly when attacked	Ensure documents and emails are seen only by authorized people	Gain visibility and control over security tools

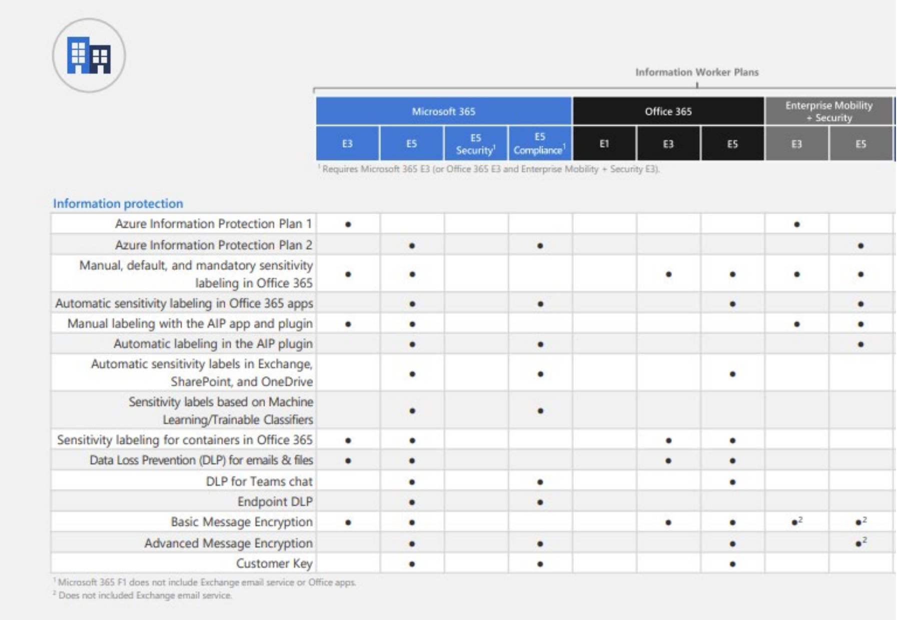
Reduce costs with an integrated solution

Secure hybrid environments effectively

Employ the world's largest and most trusted security presence

The Licensing Maze

- Microsoft’s 365 licensing can be overwhelming
  - Dozens of product bundles (E5, E3, Business Standard)
  - 400+ “Service Plans”
    - Microsoft 365 feature sets
      - E5 Information Protection & Governance
      - Azure AD Premium Plan 1
      - Microsoft Defender for Endpoint Plan 2



Information Worker Plans

	Microsoft 365				Office 365			Enterprise Mobility + Security	
	E3	E5	E5 Security[1]	E5 Compliance[1]	E1	E3	E5	E3	E5
Information protection									
Azure Information Protection Plan 1	●							●	
Azure Information Protection Plan 2		●		●					●
Manual, default, and mandatory sensitivity labeling in Office 365	●	●				●	●	●	●
Automatic sensitivity labeling in Office 365 apps		●		●			●		●
Manual labeling with the AIP app and plugin	●	●						●	●
Automatic labeling in the AIP plugin		●		●					●
Automatic sensitivity labels in Exchange, SharePoint, and OneDrive		●		●			●		
Sensitivity labels based on Machine Learning/Trainable Classifiers		●		●					
Sensitivity labeling for containers in Office 365	●	●				●	●		
Data Loss Prevention (DLP) for emails & files	●	●				●	●		
DLP for Teams chat		●		●			●		
Endpoint DLP		●		●					
Basic Message Encryption	●	●				●	●	●[2]	●[2]
Advanced Message Encryption		●		●			●		●[2]
Customer Key		●		●			●		

[1] Requires Microsoft 365 E3 (or Office 365 E3 and Enterprise Mobility + Security E3).

[1] Microsoft 365 F1 does not include Exchange email service or Office apps.

[2] Does not included Exchange email service.

Example: Retention Labeling / Policies

- A company is looking to implement retention policies and apply retention labeling across their M365 environment
- Microsoft's Answer
  - Microsoft Purview Data Lifecycle Management & Microsoft Purview Records Management
    - Formally “Microsoft Information Governance”
  - Features (Among many others):
    - Manual labeling by end users
    - Client or Server-Side Automatic labeling
    - Automatic Policies for sharing, alerting, archiving, and more
    - Standardized or custom criteria for datatypes

Retention Labeling / Policies

- Licensing
  - Per Application Retention Polices:
    - Exchange: Exchange Plan 2 or Exchange Online Archiving
    - SharePoint & OneDrive: SharePoint Plan 2
    - Teams (if policy doesn’t use adaptive scope): Microsoft 365 E5/G5/A5/E3/G3/A3/F3/F1, Business Basic, Business Standard, and Business Premium
      - Underlined if the retention or deletion period must be more than 30 days
  - Universal, cross-application retention policies and labeling
    - Microsoft 365 E5/A5/G5/E3/A3/G3
    - Microsoft 365 E5/A5/G5/F5 Compliance and F5 Security & Compliance
    - Microsoft 365 E5/A5/F5/G5 Information Protection and Governance

The Licensing Maze - Continued

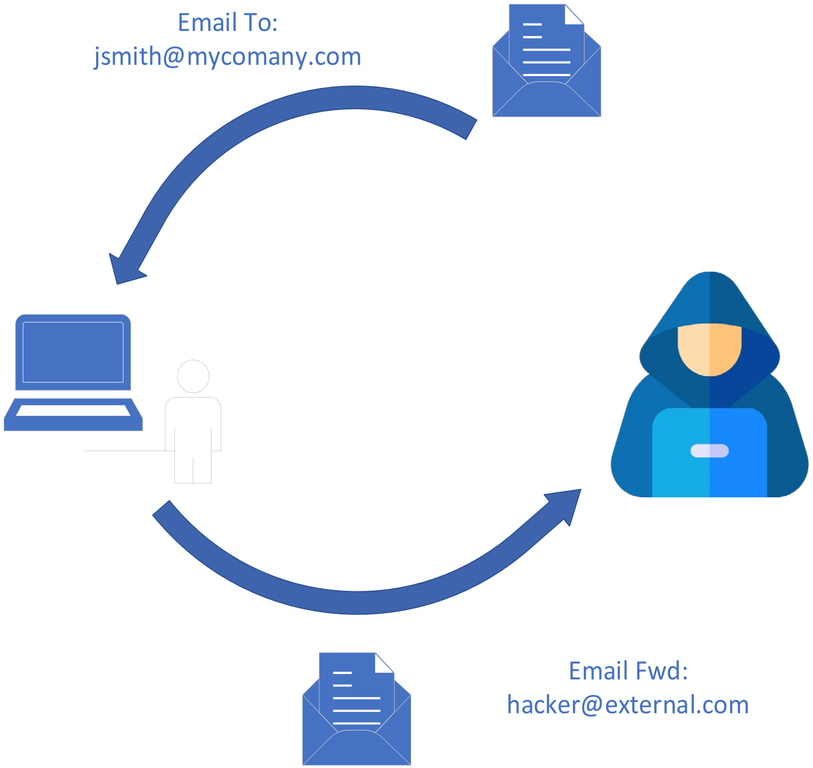
- All this can be overwhelming & convincing executives they need more $$$ can be equally difficult
- We have a 2400+ row spreadsheet to track
  - This still doesn’t cover what each setting requires only the feature set names included in each bundle
- Entire websites provide guides and matrixes to help IT admins but these often only cover the bundles

Reason 2: Dangers of the Default Config

We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Dangers of the Default Config



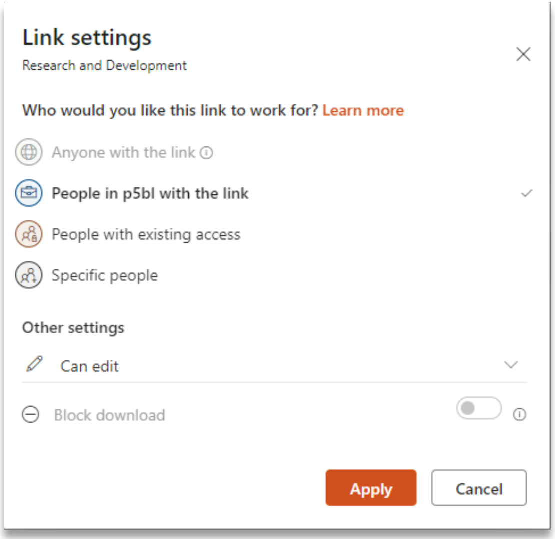
Email To:
jsmith@mycomany.com

Email Fwd:
hacker@external.com

- Microsoft has a history of promoting features over security
  - Legacy Authentication – The Bane of Business Email!
    - Used to bypass MFA enforcement
    - Finally, being removed starting October 2022!
    - Most common cause of BEC for several years now.
  - Auto forwarding – Classic Data Exfiltration
    - Used to fwd messages to outside domains without end-users knowing
    - Was originally turned on by default

The Cascade of Terribleness (Share Settings)

- Default share settings are a disaster
- Anonymous link can be sent from OneDrive and SharePoint
  - By default, these never expire!
- Any user can invite any external party as guests
  - Can be abused with anonymous links disabled
  - Guests can then share any times to anyone they choose. Even items they do not own!
- In short sharing company data is virtually unrestricted!



Link settings

Research and Development

Who would you like this link to work for? Learn more

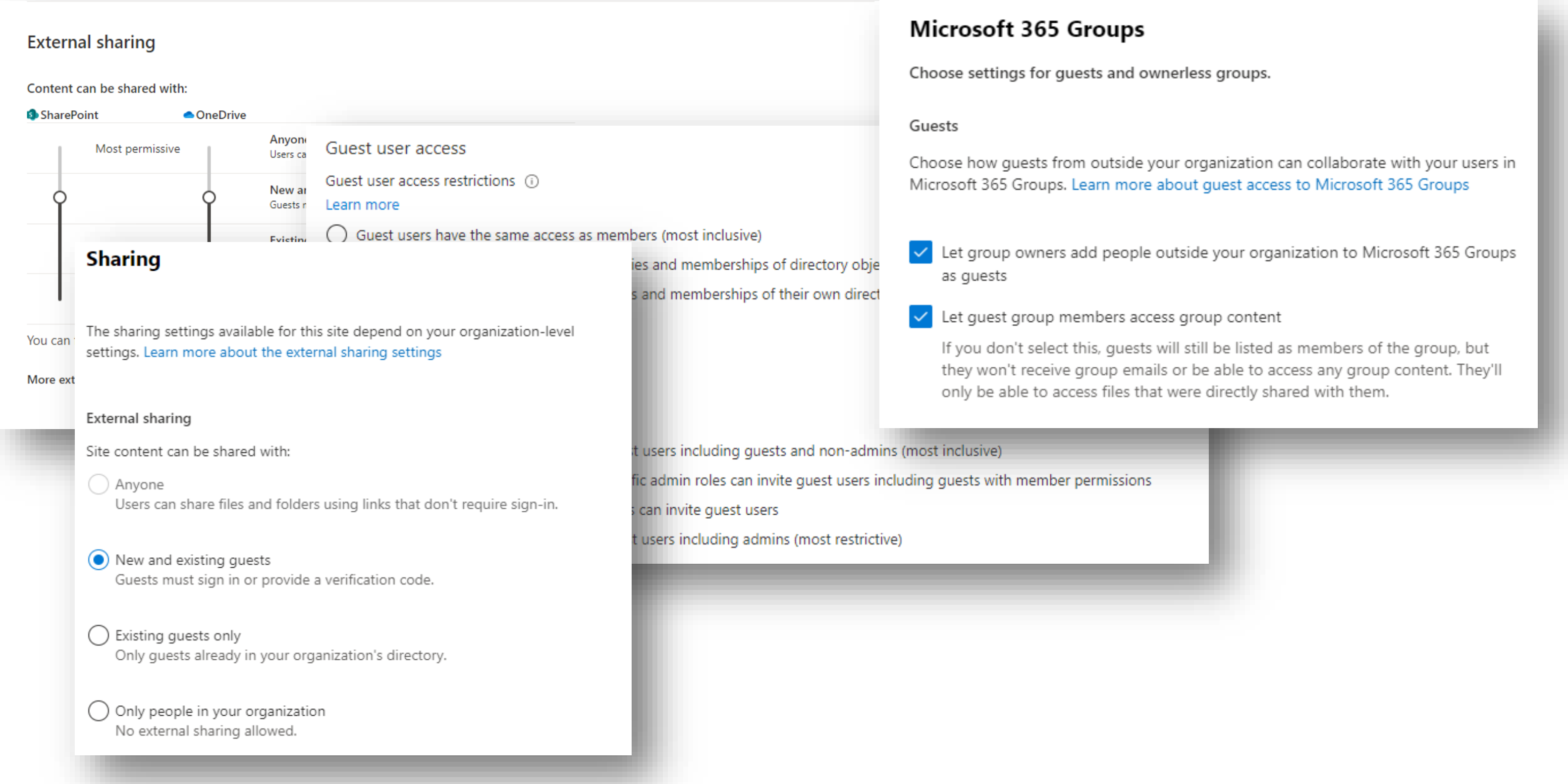
- Anyone with the link
- People in p5bl with the link ✓
- People with existing access
- Specific people

Other settings

Can edit

Block download

Guest Access Confusion



External sharing

Content can be shared with:

SharePoint OneDrive

Most permissive

Anyon
Users ca

New ar
Guests r

Existin

You can

More ext

Guest user access

Guest user access restrictions ⓘ

Learn more

○ Guest users have the same access as members (most inclusive)

ies and memberships of directory obje

s and memberships of their own direct

t users including guests and non-admins (most inclusive)

fic admin roles can invite guest users including guests with member permissions

can invite guest users

t users including admins (most restrictive)

Sharing

The sharing settings available for this site depend on your organization-level settings. Learn more about the external sharing settings

External sharing

Site content can be shared with:

○ 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
Only guests already in your organization's directory.

○ Only people in your organization
No external sharing allowed.

Microsoft 365 Groups

Choose settings for guests and ownerless groups.

Guests

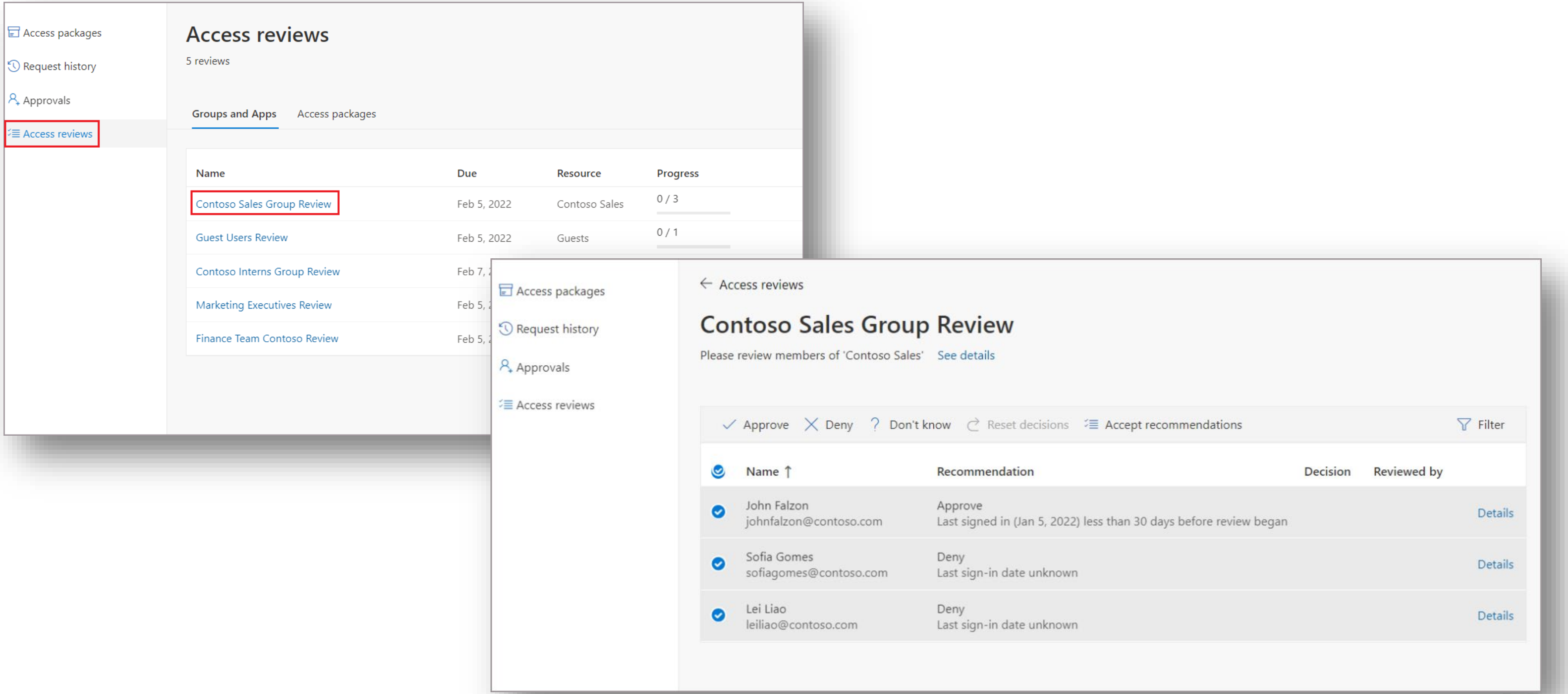
Choose how guests from outside your organization can collaborate with your users in Microsoft 365 Groups. Learn more about guest access to Microsoft 365 Groups

☑ Let group owners add people outside your organization to Microsoft 365 Groups as guests

☑ Let guest group members access group content

If you don't select this, guests will still be listed as members of the group, but they won't receive group emails or be able to access any group content. They'll only be able to access files that were directly shared with them.

Guest Access Reviews



Access reviews

5 reviews

Name	Due	Resource	Progress
Contoso Sales Group Review	Feb 5, 2022	Contoso Sales	0 / 3
Guest Users Review	Feb 5, 2022	Guests	0 / 1
Contoso Interns Group Review	Feb 7,		
Marketing Executives Review	Feb 5,		
Finance Team Contoso Review	Feb 5,		

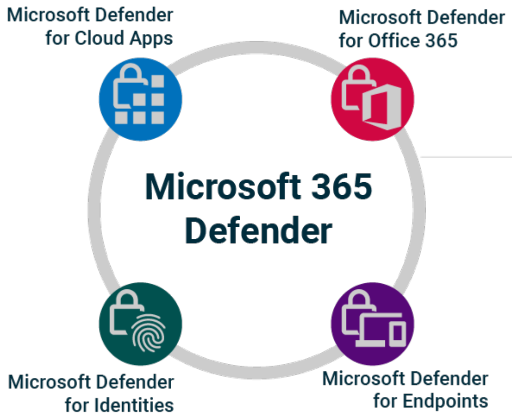
Contoso Sales Group Review

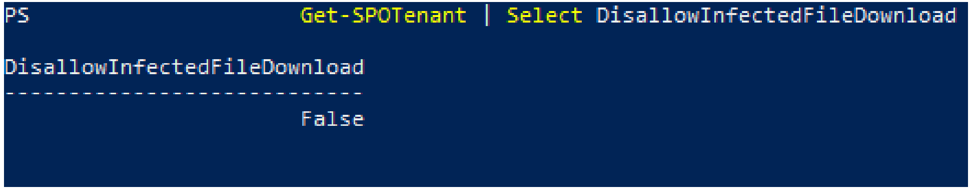
Please review members of 'Contoso Sales' See details

	Name ↑	Recommendation	Decision	Reviewed by	
✓	John Falzon johnfalzon@contoso.com	Approve Last signed in (Jan 5, 2022) less than 30 days before review began			Details
✓	Sofia Gomes sofiagomes@contoso.com	Deny Last sign-in date unknown			Details
✓	Lei Liao leiliao@contoso.com	Deny Last sign-in date unknown			Details

SharePoint Infected Files

- Microsoft 365 Defender scans SharePoint for infected files
  - With appropriate licensing
- By default it still allows users to download and share these items!


Microsoft Defender for Cloud Apps
Microsoft Defender for Office 365
Microsoft 365 Defender
Microsoft Defender for Identities
Microsoft Defender for Endpoints

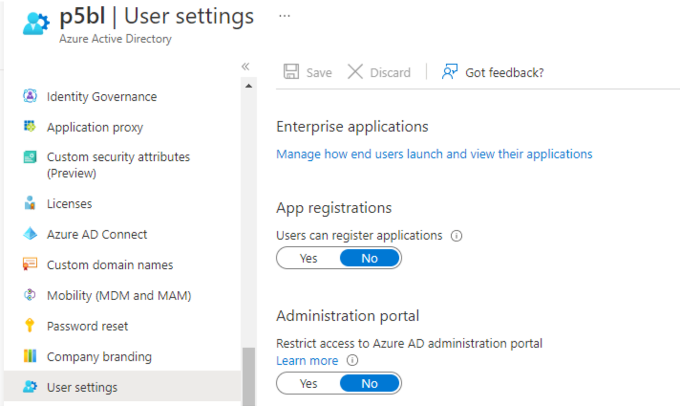


```
PS                  Get-SPOTenant | Select DisallowInfectedFileDownload

DisallowInfectedFileDownload
----------------------------
                       False
```

PowerShell & Admin portal

- Access to PowerShell & the Admin Portal is enabled for every user
- Standard users have little to no reason to use these
  - They probably don't know how!
- With these users can:
  - Enumerate all your users and groups
  - View many security configurations
  - Gain lots of valuable intel
  - Automate attacks



p5bl | User settings

Azure Active Directory

Enterprise applications

Manage how end users launch and view their applications

App registrations

Users can register applications ⓘ

Yes [✓ No]

Administration portal

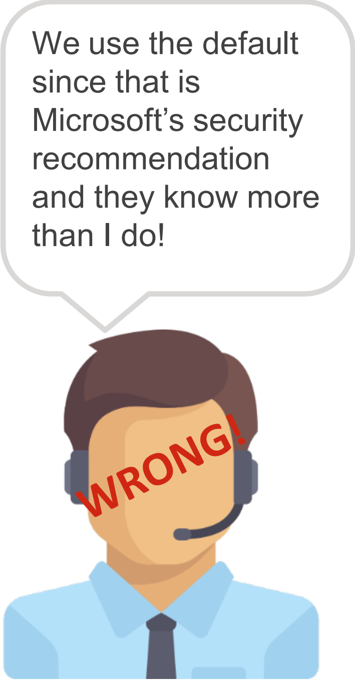
Restrict access to Azure AD administration portal

Learn more ⓘ

Yes [✓ No]

What the default config is not

- Microsoft's recommendations for securing your environment
- Highly secure configuration leaving tiny residual risk
- All Microsoft's fault
  - Microsoft cannot know business considerations, custom policies, 3rd party tools, and implementation strategies
  - Nearly every environment needs customization to truly be a reasonably secure tenant
  - The default cannot be so complex that businesses and IT can't operate


We use the default since that is Microsoft's security recommendation and they know more than I do!
WRONG!

Reason 3: IT Overload

We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

IT Overload

IT departments often don’t have the budget

- Dedicated Security Teams and M365 experts on staff cost significant $$
- IT budgets are designed to the systems running and support requests down

IT departments don’t have the time

- Microsoft 365 is a constantly changing platform and keeping up is time consuming costing valuable hours
- Settings often change in both availability and meaning
- Locations and names in the Admin Portal often change

Wrap Up

We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Conclusion

- Barriers to Microsoft 365 Security
    - Licensing and Features are complex and confusing
    - Default configurations leave much to be desired
    - IT admins have a difficult time keeping up
- IT Admins and Executives should take a moment to ask themselves or their teams a few questions

Questions to ask Yourself

- Is our current licensing sufficient and are we using the features Microsoft provides?
- Have we performed a review of our current M365 configuration with security in mind?
- Does our staff have the budget & bandwidth to keep up with the latest Microsoft changes and emerging threats?

What should you do?

- If you are already in M365- get a security review
- If you are looking to move- get some who understands these issues to harden your tenant **before** you migrate
  - ○ Unfortunately most MSPs don’t have this level of specialization

What We See

- CLA has conducted numerous M365 security reviews. Over 90% of these reviews identified at least one critical security flaw
- Examples of typical findings
  - Complete bypassing of 3rd party spam filters
  - Access Policy errors that allow multiple accounts to bypass MFA

Q & A

We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

David Sun
Principal
703-483-2650
David.Sun@CLAconnect.com

Dave Hale
Director
781-610-1228
Dave.Hale@CLAconnect.com

Nehemiah Jones
Cybersecurity Penetration Tester Senior
703-483-2661
Nehemiah.Jones@CLAconnect.com

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS