

Which Security Tool When?

A Guide To Microsoft Collaboration Security

October 2022

Microsoft
Partner



Gold Application Development
Gold Collaboration and Content
Gold Cloud Productivity
Gold Messaging
Gold Datacenter

Collaborate with Confidence

Accessible content is available upon request.

We Are AvePoint

Leader in Microsoft 365 data management solutions



 AvePoint[®] is headquartered in Jersey City, NJ, with approximately 1,500 employees across 29 offices, 14 countries, and five continents.



9M

Cloud Users



88

Countries



7

Continents

Microsoft
Partner



5x

Partner of the Year
Award Winner

AVPT

NASDAQ





Michael Wit

Senior Solutions Engineer



AvePoint Inc.



Jersey City, NJ

5 Years with AvePoint
Former Systems Administrator
100+ of Cloud Customers

Let's connect!



Michael.Wit@avepoint.com



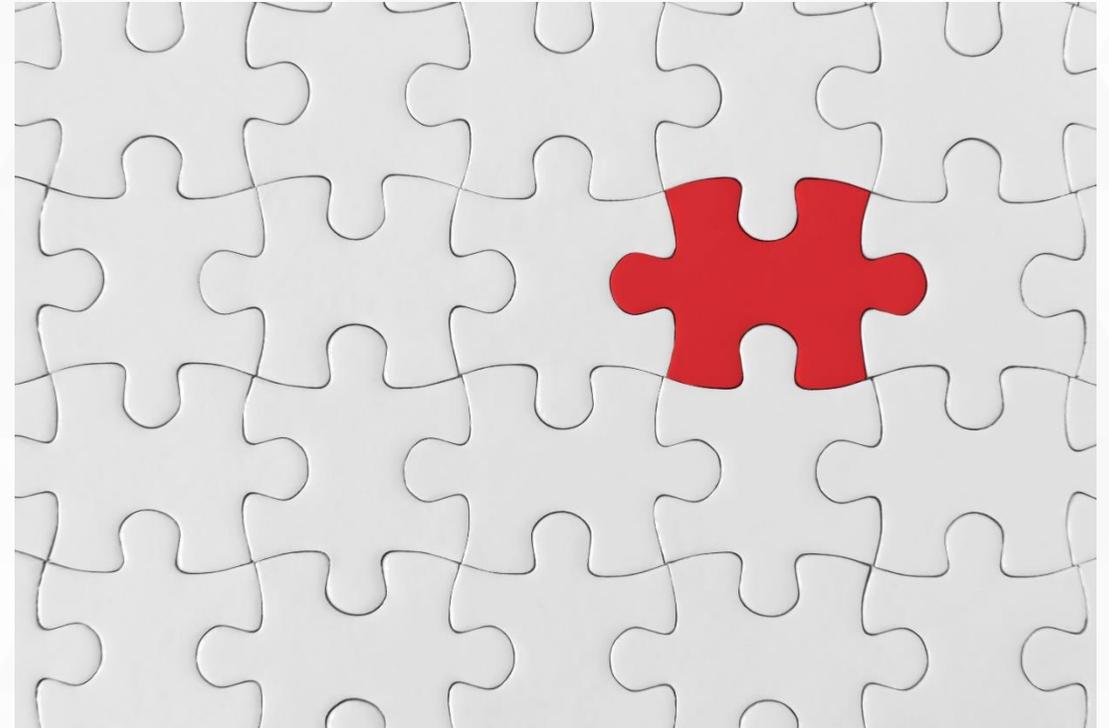
www.linkedin.com/in/mike-wit



So What Are We Talking About Today?

How the “layers” of security in M365 fit together... and where they don't!

- Securing *Identity*
- Securing *Data*
- Securing *Workspaces*
- Putting it all together...



Establishing “Identity” with Azure AD

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Home > Contoso - Overview

Contoso - Overview

Azure Active Directory

Documentation

Search (Ctrl+)

Switch directory Delete directory

Overview

Getting started

Manage

Users

Groups

Organizational relationships

Roles and administrators

Enterprise applications

Devices

App registrations

Identity Governance

Application proxy

Licenses

Azure AD Connect

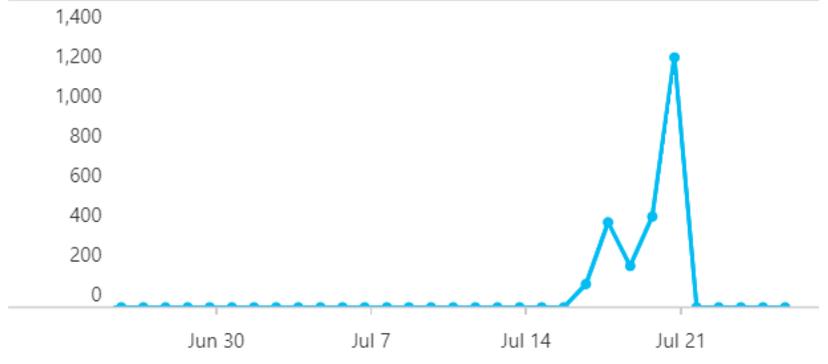
Custom domain names

M365x875773.onmicrosoft.com

Contoso

Azure AD Premium P2

Sign-ins



What's new in Azure AD

Stay up to date with the latest release notes and blog posts.

26 entries since April 20, 2018. [View archive](#)

All services (26)

New feature

Your role

Global administrator and 2 other roles [More info](#)

Find

Users

Search

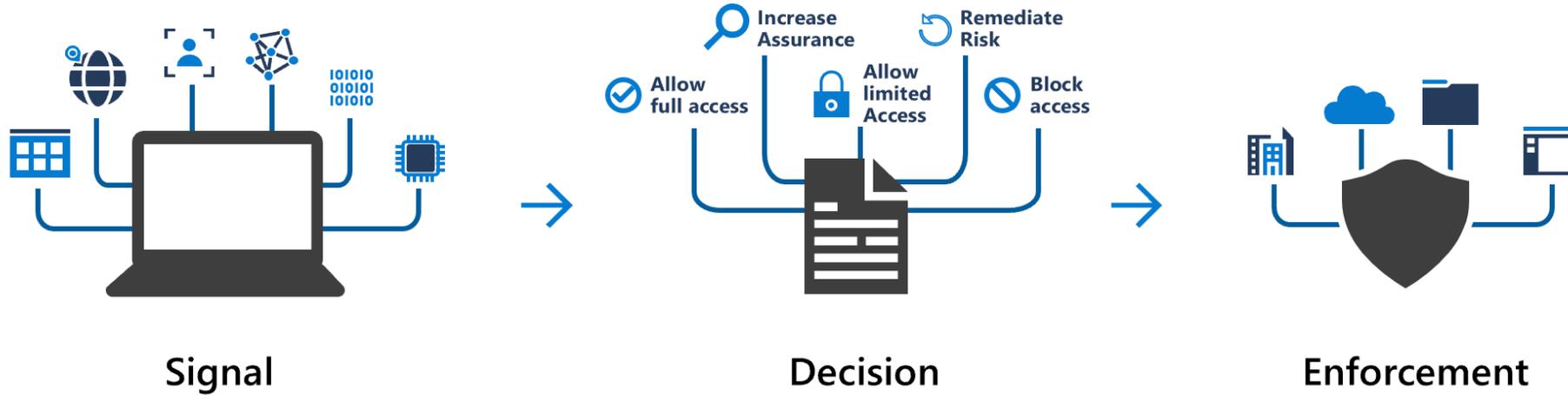
Azure AD Connect sync

Status	Not enabled
Last sync	Sync has never run

Create

- User
- Guest user
- Group

Conditional Access Overview



Phase 1

Collect Session Details

Network Location & Device
Identity

Phase 2

Enforcement

If there's a policy that is configured to block access, with the block grant control, enforcement will stop here and the user will be blocked. The user will be prompted to complete more grant control requirements that weren't satisfied during phase 1



- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor

- Home > Conditional Access - Policies
- Conditional Access - Policies
- Azure Active Directory
- Policies
- Manage
 - Named locations
 - Custom controls (preview)
 - Terms of use
 - VPN connectivity
 - Classic policies
- Troubleshooting + Support
 - Troubleshoot
 - New support request

[+ New policy](#) [What If](#) | [Got feedback?](#)

i Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. [→](#)

POLICY NAME	ENABLED
Baseline policy: Require MFA for admins (Preview)	...
Baseline policy: End user protection (Preview)	...
Baseline policy: Block legacy authentication (Preview)	...
Baseline policy: Require MFA for Service Management (Preview)	...
Require two-factor authentication for BrowserStack	✓

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Home > Conditional Access - Policies > Baseline policy: Require MFA for admins (Preview)

Baseline policy: Require MFA for admins (Preview)

Policies

Name

Baseline policy: Require MFA for admins (...)

This policy requires **multi-factor authentication (MFA)** for the following directory roles:

- Global Administrator
- SharePoint Administrator
- Exchange Administrator
- Conditional Access Administrator
- Security Administrator
- Helpdesk Administrator/Password Administrator
- Billing Administrator
- User Administrator

This policy also blocks legacy authentication.

[Learn more](#)

Enable policy

- Use policy immediately
- Do not use policy

Save

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor

Home > Conditional Access - Policies > Baseline policy: Require MFA for admins (Preview)

Baseline policy: Require M... Policies

Name
Baseline policy: Require MFA for admins (...)

This policy requires **multi-factor authentication (MFA)** for the following directory roles:

- Global Administrator
- SharePoint Administrator
- Exchange Administrator
- Conditional Access Administrator
- Security Administrator
- Helpdesk Administrator/Password Administrator
- Billing Administrator
- User Administrator

This policy also blocks legacy authentication.

[Learn more](#)

Enable policy

Use policy immediately

Do not use policy

Save

Additional Settings in Policies

Dashboard > Contoso | Security > Security | Conditional Access > Conditional Access | Policies >

CA001: Require multifactor authentication for admins ...

Conditional Access policy

Delete

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

CA001: Require multifactor authentication f...

Assignments

Users or workload identities ⓘ

[Specific users included and specific users excluded](#)

Cloud apps or actions ⓘ

[All cloud apps](#)

Conditions ⓘ

[2 conditions selected](#)

Access controls

Grant ⓘ

[1 control selected](#)

Session ⓘ

[0 controls selected](#)

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk level ⓘ

Not configured

Sign-in risk level ⓘ

Not configured

Device platforms ⓘ

[1 included and 4 excluded](#)

Locations ⓘ

Not configured

Client apps ⓘ

Not configured

Filter for devices ⓘ

[Include filtered devices](#)

Enable policy

Report-only On Off

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor

- Home > Conditional Access - Policies
- Conditional Access - Policies
Azure Active Directory
- Policies
- Manage
 - Named locations
 - Custom controls (preview)
 - Terms of use
 - VPN connectivity
 - Classic policies
- Troubleshooting + Support
 - Troubleshoot
 - New support request

[+ New policy](#)
[What If](#)
[Got feedback?](#)

Successfully updated Baseline policy: Requ... 2:54 PM
 Successfully updated Baseline policy: Require MFA for admins (Preview). Policy will be enabled in a few minutes if you have "Enable policy" set to "On".

Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. [→](#)

POLICY NAME	ENABLED	
Baseline policy: Require MFA for admins (Preview)	✓	...
Baseline policy: End user protection (Preview)		...
Baseline policy: Block legacy authentication (Preview)		...
Baseline policy: Require MFA for Service Management (Preview)		...
Require two-factor authentication for BrowserStack	✓	...

- 🏠 Home
- 📁 Sites ^
 - Active sites
 - Deleted sites
- ⚙️ Policies ^
 - Sharing
 - Access control**
- ⚙️ Settings
- 🕒 Classic features

- ☁️ OneDrive admin center
- 📁 Data migration

Access control

Use these settings to restrict how users are allowed to access content in SharePoint and OneDrive.

Unmanaged devices
Restrict access from devices that aren't compliant or joined to a domain.

Idle session sign-out
Automatically sign out users from inactive browser sessions.

Network location
Allow access only from specific IP addresses.

Apps that don't use modern authentication
Block access from Office 2010 and other apps that can't enforce device-based restrictions.



- Home
- Sites
 - Active sites
 - Deleted sites
- Policies
- Sharing
- Access control
- Settings
- Classic features
- OneDrive admin center
- Data migration

Access control

Use these settings to restrict how users are allowed to access your organization's resources.

Unmanaged devices

Restrict access from devices that aren't compliant with your organization's security requirements.

Idle session sign-out

Automatically sign out users from inactive browser sessions.

Network location

Allow access only from specific IP addresses.

Apps that don't use modern authentication

Block access from Office 2010 and other apps that don't use modern authentication.

Unmanaged devices

The setting you select here will apply to all users in your organization. To customize conditional access policies, save your selection and go to the [Azure AD admin center](#).

- Allow full access from desktop apps, mobile apps, and the web
- Allow limited, web-only access
- Block access

If you don't want to limit or block access organization-wide, you can do so for specific sites. [Learn how](#)

Save Cancel

- Home
- Sites
 - Active sites
 - Deleted sites
- Policies
- Sharing
- Access control
- Settings
- Classic features
- OneDrive admin center
- Data migration

Access control

Use these settings to restrict how users are allowed to access your organization's resources.

Unmanaged devices

Restrict access from devices that aren't compliant with your organization's security requirements.

Idle session sign-out

Automatically sign out users from inactive browser sessions.

Network location

Allow access only from specific IP addresses.

Apps that don't use modern authentication

Block access from Office 2010 and other apps that don't use modern authentication.

Unmanaged devices

i We will automatically change the "Apps that don't use modern authentication" setting to block access (because these apps can't enforce this device-based restriction).

The setting you select here will apply to all users in your organization. To customize conditional access policies, save your selection and go to the [Azure AD admin center](#).

- Allow full access from desktop apps, mobile apps, and the web
- Allow limited, web-only access
- Block access

If you don't want to limit or block access organization-wide, you can do so for specific sites. [Learn how](#)

Save

Cancel

- 🏠 Home
- 📁 Sites ^
 - Active sites
 - Deleted sites
- ⚙️ Policies ^
- Sharing
- Access control**
- ⚙️ Settings
- 🕒 Classic features

- ☁️ OneDrive admin center
- 📁 Data migration

Access control

Use these settings to restrict how users are allowed to access content in SharePoint and OneDrive.

Unmanaged devices
Restrict access from devices that aren't compliant or joined to a domain.

Idle session sign-out
Automatically sign out users from inactive browser sessions.

Network location
Allow access only from specific IP addresses.

Apps that don't use modern authentication
Block access from Office 2010 and other apps that can't enforce device-based restrictions.



- + Create a resource
- 🏠 Home
- 📊 Dashboard
- ☰ All services
- ★ FAVORITES
- 📁 All resources
- 📁 Resource groups
- 🔄 App Services
- ⚡ Function App
- 📊 SQL databases
- 🌌 Azure Cosmos DB
- 🖥️ Virtual machines
- ⚖️ Load balancers
- 📀 Storage accounts
- 🌐 Virtual networks
- 🔑 Azure Active Directory
- 📈 Monitor
- 🗨️ Advisor

Home > Contoso > Conditional Access - Policies

Conditional Access - Policies

Azure Active Directory

☰ Policies

Manage

- 🔗 Named locations
 - 🔧 Custom controls (preview)
 - ✅ Terms of use
 - ⚙️ VPN connectivity
 - ☰ Classic policies
-
- #### Troubleshooting + Support
- 🔧 Troubleshoot
 - 🗨️ New support request

+ New policy | 👤 What If | ❤️ Got feedback?

📘 Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. →

POLICY NAME	ENABLED	
Baseline policy: Require MFA for admins (Preview)	✓	...
Baseline policy: End user protection (Preview)		...
Baseline policy: Block legacy authentication (Preview)		...
Baseline policy: Require MFA for Service Management (Preview)		...
Require two-factor authentication for BrowserStack	✓	...
[SharePoint admin center]Use app-enforced Restrictions for browser access - 201...	✓	...

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor

Home > Contoso > Conditional Access - Policies

Conditional Access - Policies

Azure Active Directory

Policies

Manage

- Named locations
- Custom controls (preview)
- Terms of use
- VPN connectivity
- Classic policies
- Troubleshooting + Support
- Troubleshoot
- New support request

+ New policy | What If | Got feedback?

Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. →

POLICY NAME	ENABLED	
Baseline policy: Require MFA for admins (Preview)	✓	...
Baseline policy: End user protection (Preview)		...
Baseline policy: Block legacy authentication (Preview)		...
Baseline policy: Require MFA for Service Management (Preview)		...
Require two-factor authentication for BrowserStack	✓	...
[SharePoint admin center]Use app-enforced Restrictions for browser access - 201...	✓	...

✓ Successfully updated [SharePoint admin c... 3:45 PM

Successfully updated [SharePoint admin center]Use app-enforced Restrictions for browser access - 2019/07/26. Policy will be enabled in a few minutes if you have "Enable policy" set to "On".

Install Office

Good afternoon


Start new


Outlook


OneDrive


Word


Excel


PowerPoint


OneNote


SharePoint


Teams


Yammer


Admin


All apps

Recommended



 You edited this
Sun at 4:50 AM



Product Launch

 You edited this
Sun at 4:44 AM



Marketing Deck v1

 You edited this
Sun at 4:51 AM



Fabrikam3DPrinterBrochure

 You edited this
Sun at 4:43 AM



Introducin



Access Denied

Due to organizational policies, you can't access this resource from this untrusted device.

Here are a few ideas:

-  Please contact your organization.

If this problem persists, contact your support team and include these technical details:

Correlation ID: d22af49e-6005-0000-40ff-2eca6e97090b

Date and Time: 7/26/2019 3:56:49 PM

Issue Type: User has encountered a policy issue.

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Home > Contoso > Conditional Access - Policies

Conditional Access - Policies

Azure Active Directory

Policies

Manage

Named locations

Custom controls (preview)

Terms of use

VPN connectivity

Classic policies

Troubleshooting + Support

Troubleshoot

New support request

+ New policy | What If | Got feedback?

Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. →

POLICY NAME	ENABLED	
Baseline policy: Require MFA for admins (Preview)	✓	...
Baseline policy: End user protection (Preview)		...
Baseline policy: Block legacy authentication (Preview)		...
Baseline policy: Require MFA for Service Management (Preview)		...
Require two-factor authentication for BrowserStack	✓	...
[SharePoint admin center]Use app-enforced Restrictions for browser access - 201...	✓	...

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor

Home > Contoso > Conditional Access - Terms of use

Conditional Access - Terms of use

Azure Active Directory

- Polices
- Manage
 - Named locations
 - Custom controls (preview)
 - Terms of use**
 - VPN connectivity
 - Classic policies
- Troubleshooting + Support
 - Troubleshoot
 - New support request

[+ New terms](#)
[Edit terms](#)
[Delete terms](#)
[View audit logs](#)
[View selected audit logs](#)
More

Search for a terms of use

NAME	ACCEPTED	DECLINED
No terms of use to display		

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Home > Contoso > Conditional Access - Terms of use > New terms of use

New terms of use

Terms of use

Create and upload documents

* Name ⓘ

* Display name ⓘ

Terms of use document ⓘ ▼

+ Add language

Require users to expand the terms of use ⓘ

Require users to consent on every device ⓘ

Expire consents ⓘ

Duration before re-acceptance required (days) ⓘ

Conditional access

Create

Microsoft Azure

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor

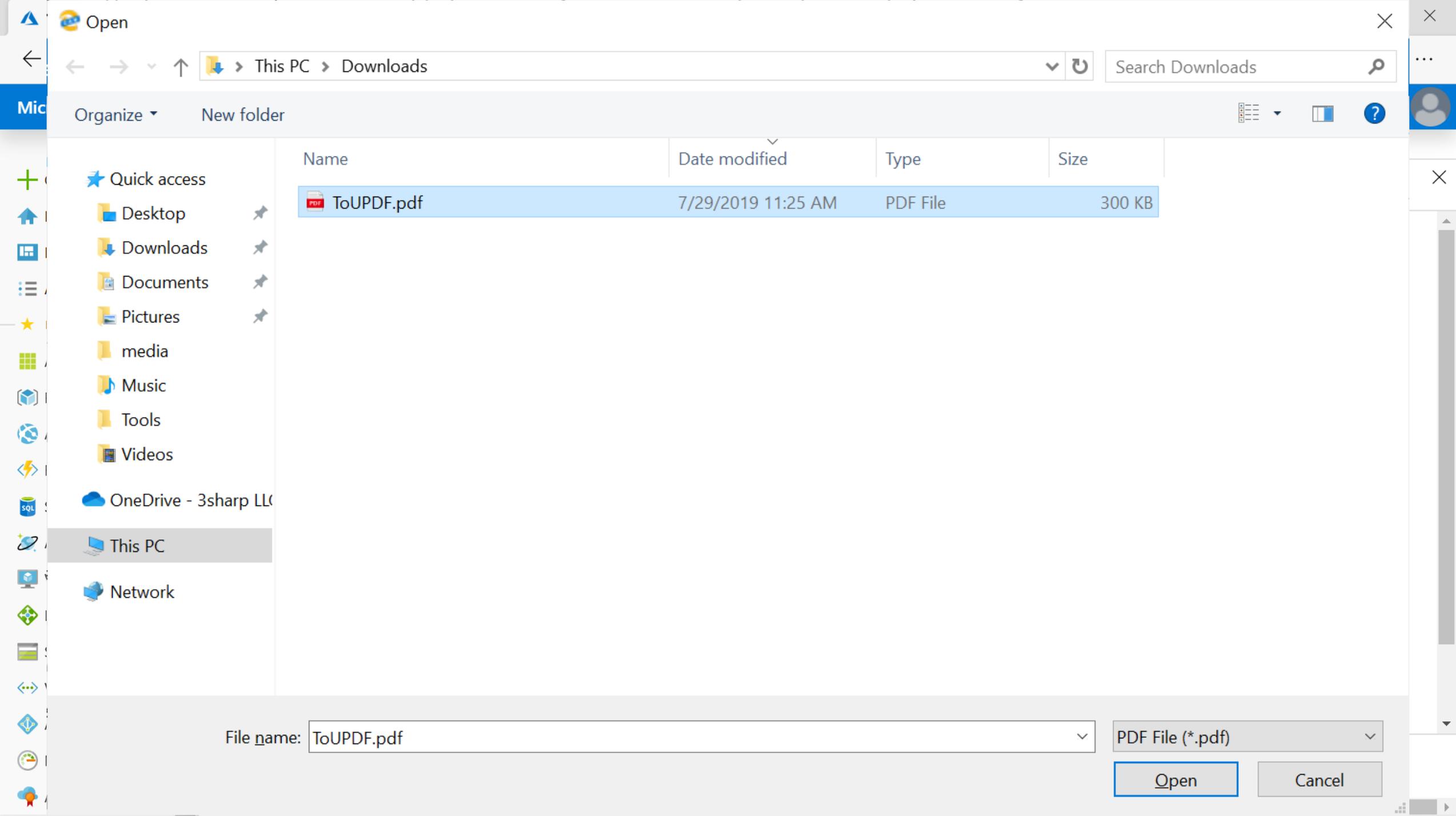
Open This PC > Downloads Search Downloads

Organize New folder

Name	Date modified	Type	Size
<ul style="list-style-type: none"> Quick access Desktop Downloads Documents Pictures media Music Tools Videos OneDrive - 3sharp LLC This PC Network 			
ToUPDF.pdf	7/29/2019 11:25 AM	PDF File	300 KB

File name: PDF File (*.pdf)

Create



Open

This PC > Downloads

Search Downloads

Organize

New folder

Quick access

Desktop

Downloads

Documents

Pictures

media

Music

Tools

Videos

OneDrive - 3sharp LLC

This PC

Network

Name

Date modified

Type

Size

ToUPDF.pdf

7/29/2019 11:25 AM

PDF File

300 KB

File name: ToUPDF.pdf

PDF File (*.pdf)

Open

Cancel

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Home > Contoso > Conditional Access - Terms of use > New terms of use

New terms of use

Terms of use

Create and upload documents

* Name ⓘ

* Display name ⓘ

Terms of use document ⓘ 

+ Add language

Require users to expand the terms of use ⓘ On Off

Require users to consent on every device ⓘ On Off

Expire consents ⓘ On Off

Duration before re-acceptance required (days) ⓘ

Conditional access

Create

Upload Completed for ToUPDF.pdf 11:45 AM

299.66 KiB | "Streaming upload"

Search resources, services, and docs

Microsoft Azure

Home > Contoso > Conditional Access - Terms of use

Conditional Access - Terms of use

Azure Active Directory

✔ Create terms of use "Contoso Terms of Us... 11:57 AM
Successfully created terms of use "Contoso Terms of Use Policy"

Polices

Manage

- Named locations
 - Custom controls (preview)
 - Terms of use**
 - VPN connectivity
 - Classic policies
- Troubleshooting + Support
- Troubleshoot
 - New support request

+ New terms Edit terms Delete terms View audit logs View selected audit logs More

Search for a terms of use

NAME	ACCEPTED	DECLINED
Contoso Terms of Use Policy	0	0

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor

- + Create a resource
- 🏠 Home
- 📊 Dashboard
- ☰ All services
- ★ FAVORITES
- 📄 All resources
- 📁 Resource groups
- 🔄 App Services
- ⚡ Function App
- 🗄️ SQL databases
- 🌌 Azure Cosmos DB
- 💻 Virtual machines
- ⚖️ Load balancers
- 📀 Storage accounts
- 🌐 Virtual networks
- 🔑 Azure Active Directory
- 📈 Monitor
- 🗣️ Advisor

Home > Contoso > Conditional Access - Policies

Conditional Access - Policies

Azure Active Directory

☰ Policies

Manage

- 📍 Named locations
- 🔧 Custom controls (preview)
- ✅ Terms of use
- ⚙️ VPN connectivity
- ☰ Classic policies

Troubleshooting + Support

- 🔧 Troubleshoot
- 🗣️ New support request

+ New policy | 👤 What If | ❤️ Got feedback?

📘 Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. →

POLICY NAME	ENABLED	
Baseline policy: Require MFA for admins (Preview)	✓	...
Baseline policy: End user protection (Preview)		...
Baseline policy: Block legacy authentication (Preview)		...
Baseline policy: Require MFA for Service Management (Preview)		...
Require two-factor authentication for BrowserStack	✓	...
[SharePoint admin center]Use app-enforced Restrictions for browser access - 201...	✓	...

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor

Home > Contoso > Conditional Access - Policies > New > Users and groups

New

Info

* Name
External User Saas Apps Terms of Use P... ✓

Assignments

Users and groups ⓘ
0 users and groups selected

Cloud apps or actions ⓘ
No cloud apps or actions sele...

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
0 controls selected

Session ⓘ

Create

Users and groups

Include Exclude

None

All users

Select users and groups

All guest and external users (preview) ⓘ

Directory roles (preview) ⓘ

Users and groups

Done

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Home > Contoso > Conditional Access - Policies > New > Cloud apps or actions

New

Info

* Name

External User Saas Apps Terms of Use P... ✓

Assignments

Users and groups ⓘ
Specific users included >

Cloud apps or actions ⓘ
No cloud apps or actions sele... >

Conditions ⓘ
0 conditions selected >

Access controls

Grant ⓘ
0 controls selected >

Session ⓘ

Create

Cloud apps or actions

Select what this policy applies to

Cloud apps User actions

Include Exclude

- None
- All cloud apps
- Select apps

Done

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor

Home > Contoso > Conditional Access - Policies > New > Cloud apps or actions

New

Info

* Name
External User Saas Apps Terms of Use P... ✓

Assignments

Users and groups ⓘ
Specific users included >

Cloud apps or actions ⓘ
No cloud apps or actions sele... >

Conditions ⓘ
0 conditions selected >

Access controls

Grant ⓘ
0 controls selected >

Session ⓘ

Create

Cloud apps or actions

Select what this policy applies to

Cloud apps User actions

Include Exclude

None

All cloud apps

Select apps

Select
None >

Done

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Home > Contoso > Conditional Access - Policies > New > Cloud apps or actions > Select

New

Info

* Name

External User Saas Apps Terms of Use P... ✓

Assignments

Users and groups ⓘ

Specific users included >

Cloud apps or actions ⓘ

No cloud apps or actions sele... >

Conditions ⓘ

0 conditions selected >

Access controls

Grant ⓘ

0 controls selected >

Session ⓘ

Create

Cloud apps or actions

Select what this policy applies to

Cloud apps User actions

Include Exclude

- None
- All cloud apps
- Select apps

Select
None >

Done

Select

Cloud apps

Applications ⓘ

Search Applications... ✓

-  Azure Advanced Threat Protection
-  Azure Analysis Services
-  Box
-  BrowserStack
-  Microsoft Azure Information Prot
-  Microsoft Azure Management

Selected
None >

Select

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

New

Info

* Name

External User Saas Apps Terms of Use P... ✓

Assignments

Users and groups ⓘ

Specific users included >

Cloud apps or actions ⓘ

No cloud apps or actions sele... >

Conditions ⓘ

0 conditions selected >

Access controls

Grant ⓘ

0 controls selected >

Session ⓘ

Create

Cloud apps or actions

Select what this policy applies to

Cloud apps User actions

Include Exclude

- None
- All cloud apps
- Select apps

Select
None >

Done

Select

Cloud apps

Applications ⓘ

Search Applications... ✓



Office Sway



Outlook Groups



Power BI Service



Salesforce



Skype for Business Online

Selected >

None

Select

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Home > Contoso > Conditional Access - Policies > New > Grant

New

Info

* Name

External User Saas Apps Terms of Use P... ✓

Assignments

Users and groups ⓘ
Specific users included >

Cloud apps or actions ⓘ
1 app included >

Conditions ⓘ
0 conditions selected >

Access controls

Grant ⓘ
0 controls selected >

Session ⓘ

Create

Grant

Select the controls to be enforced.

- Block access
- Grant access
- Require multi-factor authentication ⓘ
- Require device to be marked as compliant ⓘ
- Require Hybrid Azure AD joined device ⓘ
- Require approved client app ⓘ
[See list of approved client apps](#)
- Require app protection policy (preview) ⓘ
[See list of policy protected client apps](#)
- Contoso Terms of Use Policy

Select

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Home > Contoso > Conditional Access - Policies > New > Grant

New

Info

* Name

External User Saas Apps Terms of Use P... ✓

Assignments

Users and groups ⓘ
Specific users included >

Cloud apps or actions ⓘ
1 app included >

Conditions ⓘ
0 conditions selected >

Access controls

Grant ⓘ
0 controls selected >

Session ⓘ

Create

Grant

Select the controls to be enforced.

- Block access
- Grant access
- Require multi-factor authentication ⓘ
- Require device to be marked as compliant ⓘ
- Require Hybrid Azure AD joined device ⓘ
- Require approved client app ⓘ
[See list of approved client apps](#)
- Require app protection policy (preview) ⓘ
[See list of policy protected client apps](#)
- Contoso Terms of Use Policy

Select

Conditional Access - Policies

Azure Active Directory

- + Create a resource
- 🏠 Home
- 📊 Dashboard
- ☰ All services
- ★ FAVORITES
- 📁 All resources
- 📁 Resource groups
- 🔄 App Services
- ⚡ Function App
- 📊 SQL databases
- 🌌 Azure Cosmos DB
- 🖥️ Virtual machines
- ⚖️ Load balancers
- 📁 Storage accounts
- 🌐 Virtual networks
- 🔑 Azure Active Directory
- 📈 Monitor
- 🗨️ Advisor

- ☰ Policies
- Manage
 - 🌐 Named locations
 - 🔧 Custom controls (preview)
 - ✅ Terms of use
 - ⚙️ VPN connectivity
 - ☰ Classic policies
- Troubleshooting + Support
 - 🔧 Troubleshoot
 - 👤 New support request

+ New policy | 👤 What If | ❤️ Got feedback?

📘 Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. →

POLICY NAME	ENABLED	
Baseline policy: Require MFA for admins (Preview)	✓	...
Baseline policy: End user protection (Preview)		...
Baseline policy: Block legacy authentication (Preview)		...
Baseline policy: Require MFA for Service Management (Preview)		...
Require two-factor authentication for BrowserStack	✓	...
[SharePoint admin center]Use app-enforced Restrictions for browser access - 201...	✓	...
External User Saas Apps Terms of Use Policy	✓	...

Apps



Add-In



Calendar



Excel



Kaizala



OneDrive



People



PowerApps



Box



Delve



Flow



LinkedIn



OneNote



Planner



PowerPoint



BrowserStack



Dynamics 365



Forms



MyAnalytics



Outlook



Power BI



Salesforce



Groups



Access reviews



Contoso Terms of Use

In order to access Contoso resource(s), you must read the Terms of Use.

Contoso Terms of Use >

Please click Accept to confirm that you have read and understood the terms of use.



Contoso Terms of Use

In order to access Contoso resource(s), you must read the Terms of Use.

Contoso Terms of Use >

Please click Accept to confirm that you have

Decline Accept

Just a sec...

 You must view the terms of use before you can accept.

Ok



Contoso Terms of Use

In order to access Contoso resource(s), you must read the Terms of Use.

Contoso Terms of Use >

Please click Accept to confirm that you have read and understood the terms of use.



Contoso Terms of Use

In order to access Contoso resource(s), you must read the Terms of Use.

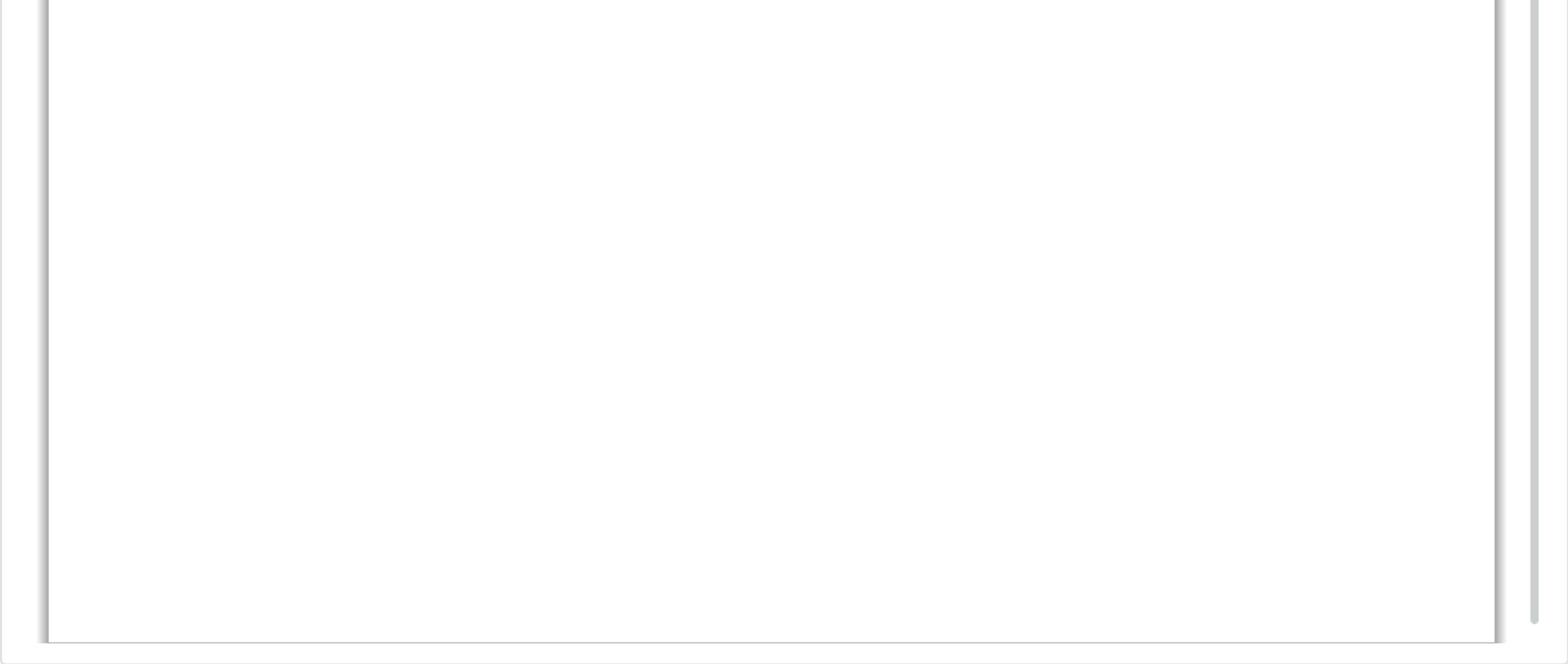
Contoso Terms of Use

Zoom out Zoom in Reset zoom

Contoso, Ltd.

Terms of Use
Cloud Applications

By accessing this portal and all associated Contoso, Ltd. cloud-based applications you agree to all Contoso, Ltd. IT policies as outlined in the Contoso, Ltd. employee handbook.



Please click Accept to confirm that you have read and understood the terms of use.

What is Azure AD B2B and “External Identities”?



External access to SharePoint, Groups and Teams is “on by default” in M365 and “open for business”

Turn on or turn off guest access to Microsoft Teams

01/08/2021 • 3 minutes to read •  • Applies to: Microsoft Teams

Note

Until **February 2021**, guest access is turned off by default. You must turn on guest access for Teams before admins or team owners can add guests. After you turn on guest access, it might take a few hours for the changes to take effect. If users see the message **Contact your administrator** when they try to add a guest to their team, it's likely that either guest access hasn't been turned on or the settings aren't effective yet.

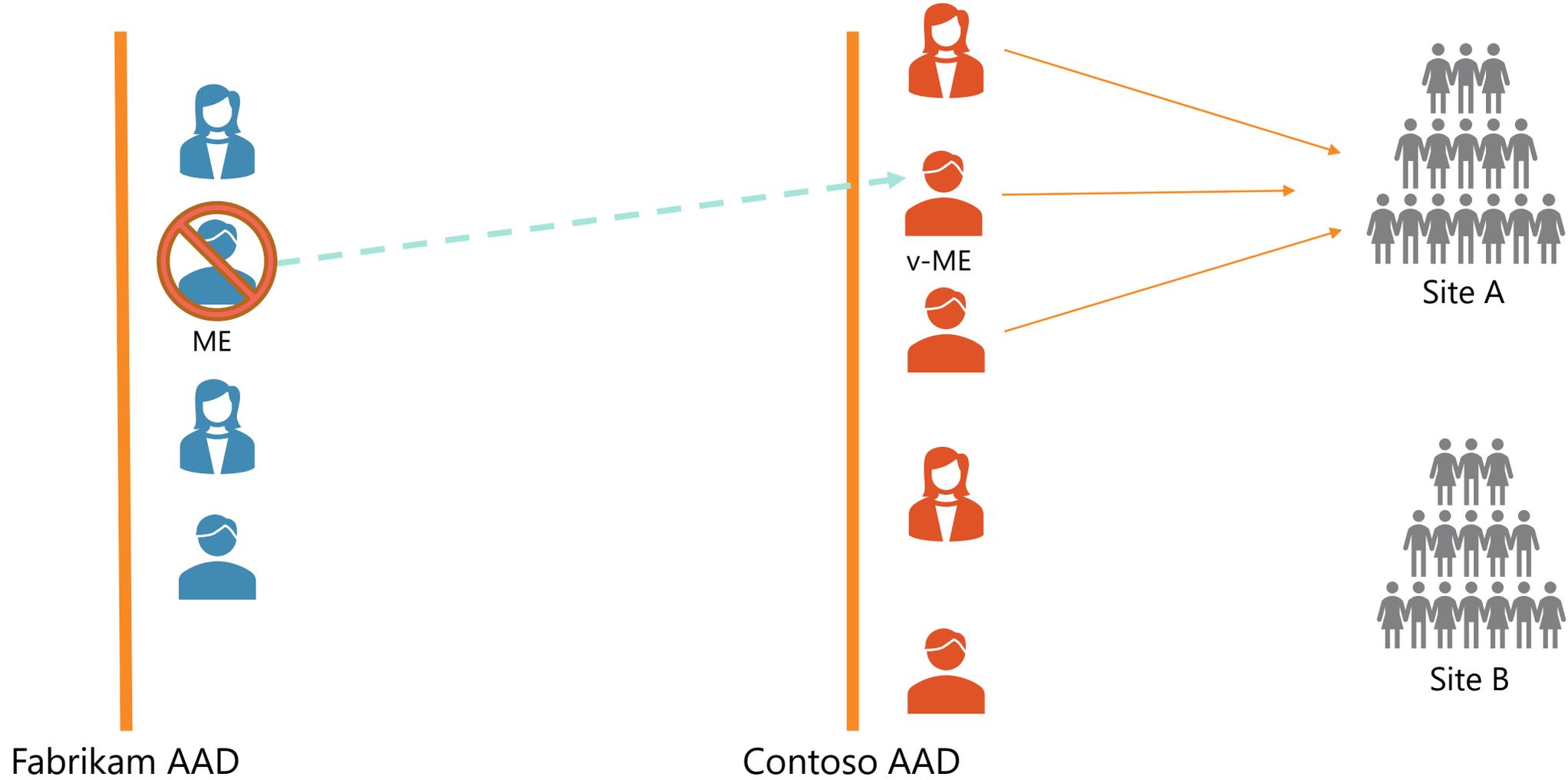
After February 2021, guest access in Microsoft Teams will be turned on by default for new customers & existing customers who haven't configured this setting. When this change is implemented, if you've not already configured guest access capability in Microsoft Teams, that capability will be enabled in your tenant. If you want guest access to remain disabled for your organization, you'll need to confirm that the guest access setting is set to **Off** instead of **Service default**.

Understanding the Azure AD “Guest” Model

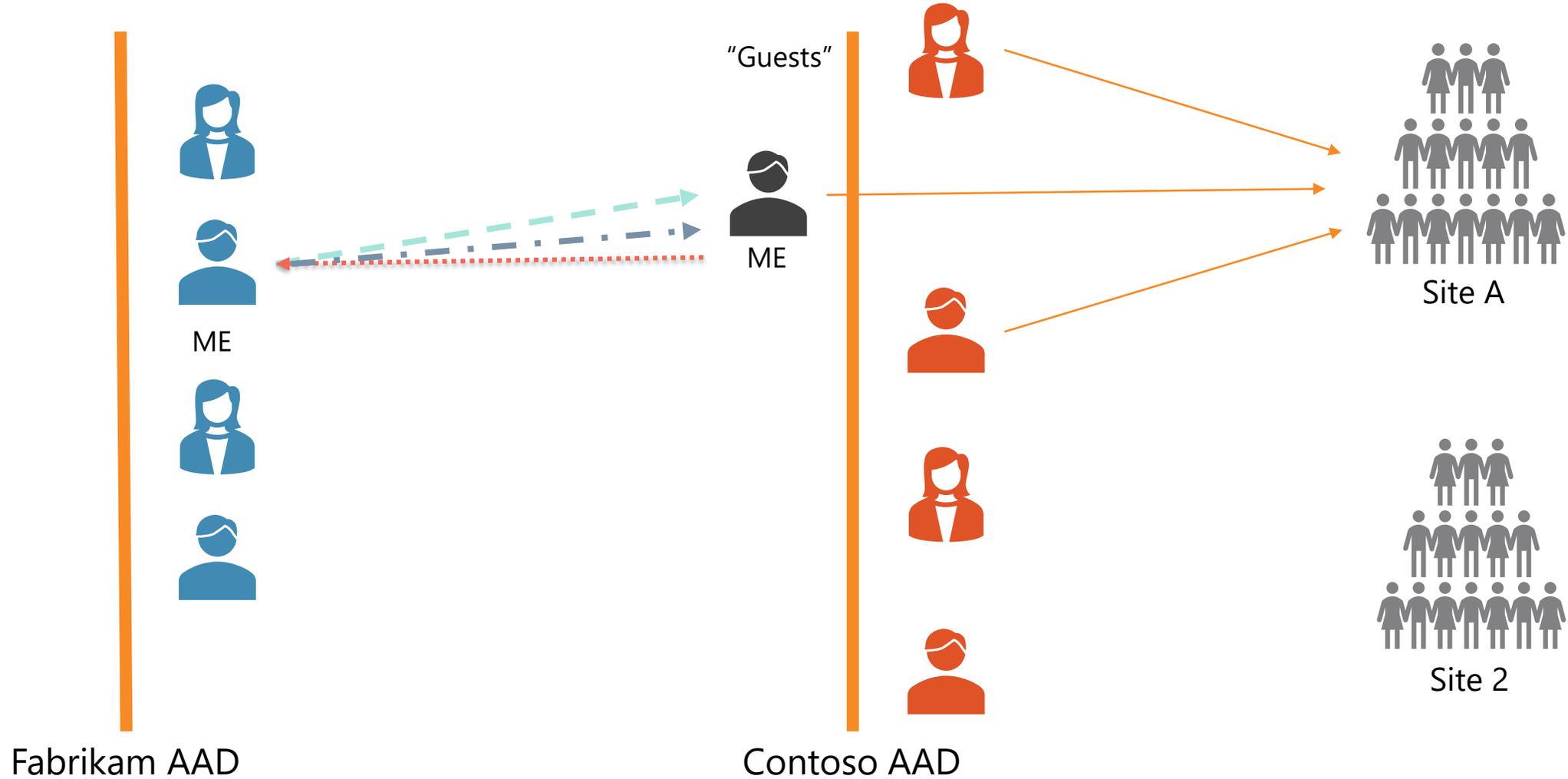
The foundation of
external collaboration
in Teams



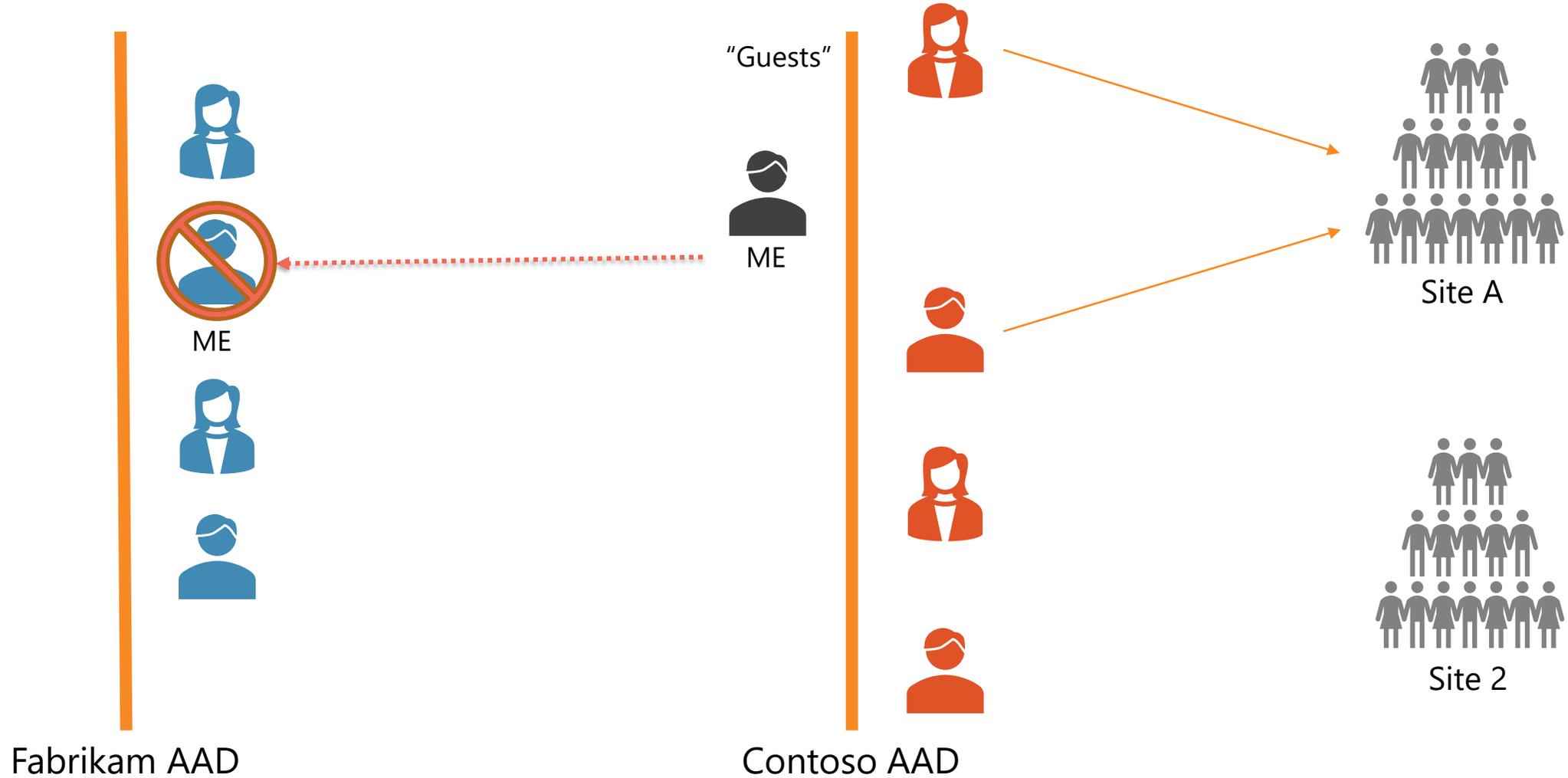
"In the beginning..."



The Azure B2B Guest Model



The Azure B2B Guest Model



Benefits of the AAD B2B approach?



- Home domain authenticates user
- Guest domain can leverage AAD conditional access policies
- Centralized identity in guest means centralized reporting or memberships



← Guest User & External Access
eBook



Configuring B2B settings in AAD...

The screenshot displays the Azure Active Directory admin center interface. The left-hand navigation pane includes sections for Dashboard, All services, FAVORITES (Azure Active Directory, Users, Enterprise applications), Self-service sign up (Custom user attributes, All API connectors, User flows), Subscriptions (Linked subscriptions), Lifecycle management (Terms of use, Access reviews), and Troubleshooting + Support (New support request). The main content area is titled 'External Identities | External collaboration settings' for the 'Contoso - Azure Active Directory' tenant. It features a search bar, 'Save' and 'Discard' buttons, and several configuration sections: 'Guest user access restrictions (Preview)' with three radio button options (the second is selected); 'Guest invite settings' with three toggle switches (all are set to 'Yes'); and 'Collaboration restrictions' with three radio button options (the second is selected).

Azure Active Directory admin center

Dashboard > Contoso > External Identities

External Identities | External collaboration settings

Contoso - Azure Active Directory

Search (Ctrl+/) << Save Discard

Get started

All identity providers

External collaboration settings

Diagnose and solve problems

Self-service sign up

Custom user attributes (Preview)

All API connectors (Preview)

User flows (Preview)

Subscriptions

Linked subscriptions

Lifecycle management

Terms of use

Access reviews

Troubleshooting + Support

New support request

Guest user access restrictions (Preview) ⓘ

[Learn more](#)

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

Guest users have limited access to properties and memberships of directory objects

Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Admins and users in the guest inviter role can invite ⓘ

Yes No

Members can invite ⓘ

Yes No

Guests can invite ⓘ

Yes No

Enable Email One-Time Passcode for guests (Preview) ⓘ

[Learn more](#)

Yes No

Enable guest self-service sign up via user flows (Preview) ⓘ

[Learn more](#)

Yes No

Collaboration restrictions

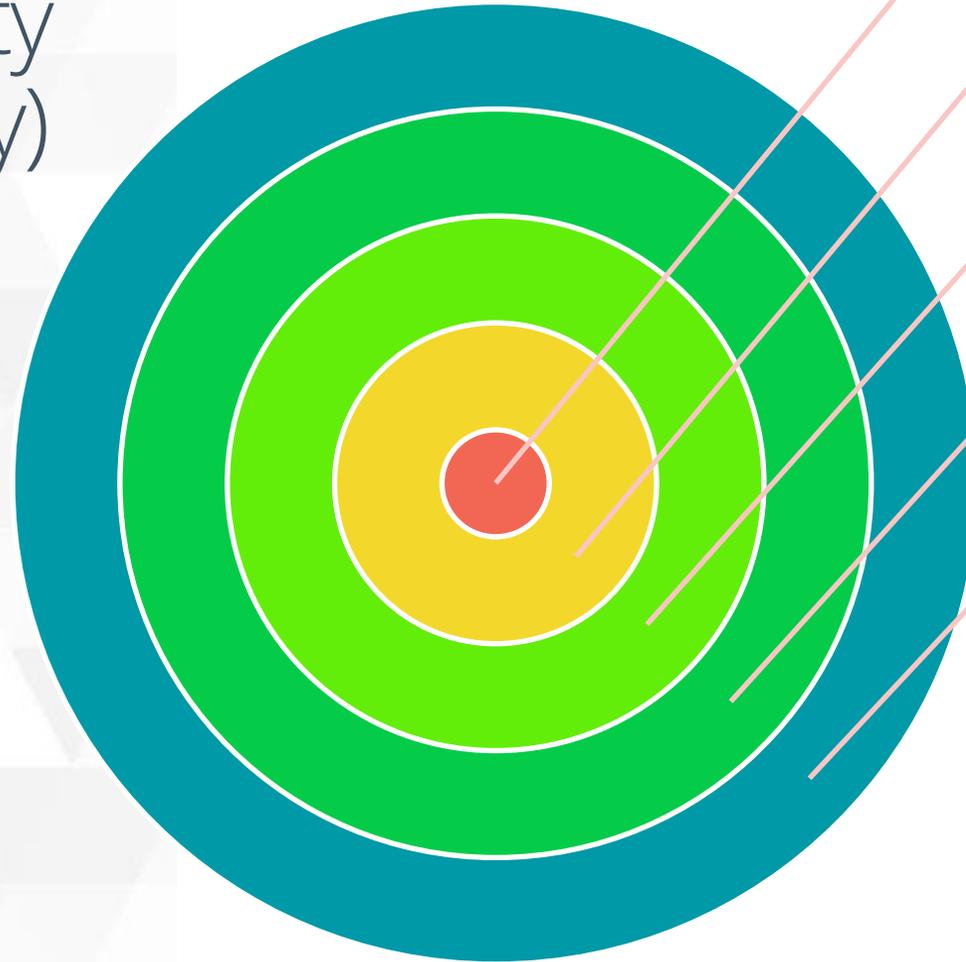
Allow invitations to be sent to any domain (most inclusive)

Deny invitations to the specified domains

Allow invitations only to the specified domains (most restrictive)



Layered settings
provide flexibility
(and complexity)



AAD Settings

• *Lots of options*

O365 Security and Privacy Setting

• *On/Off*

Group Settings

• *2 Options*

SharePoint setting

Teams Settings

• *Many options*

O365 Tenant wide: Owners can invite new guests?

The screenshot shows the Microsoft 365 admin center for Contoso Electronics. The left sidebar contains navigation options: Home, Users, Groups, Roles, Resources, Billing, Support, Settings, Domains, Microsoft Search, Org settings, Add-ins, Partner relationships, Setup, Reports, and Health. The main content area is titled 'Org settings' and has tabs for Services, Security & privacy (selected), and Organization profile. A table lists various settings, with 'Sharing' highlighted. The 'Sharing' setting is described as 'Control access for people outside'.

Name ↑	Description
Customer lockbox	Set requirements for data access.
Password expiration policy	Set the password policy for all use
Privacy profile	Set the privacy statement of your
Privileged access	Set scoped access for privilege ta
Self-service password reset	Let users reset their own forgotte
Sharing	Control access for people outside

Sharing

When this setting is selected, all users can add people outside the organization as guests, so they appear on the Guest users page. When this setting isn't selected, only admins can add guests. [Learn more about guests in your organization.](#)

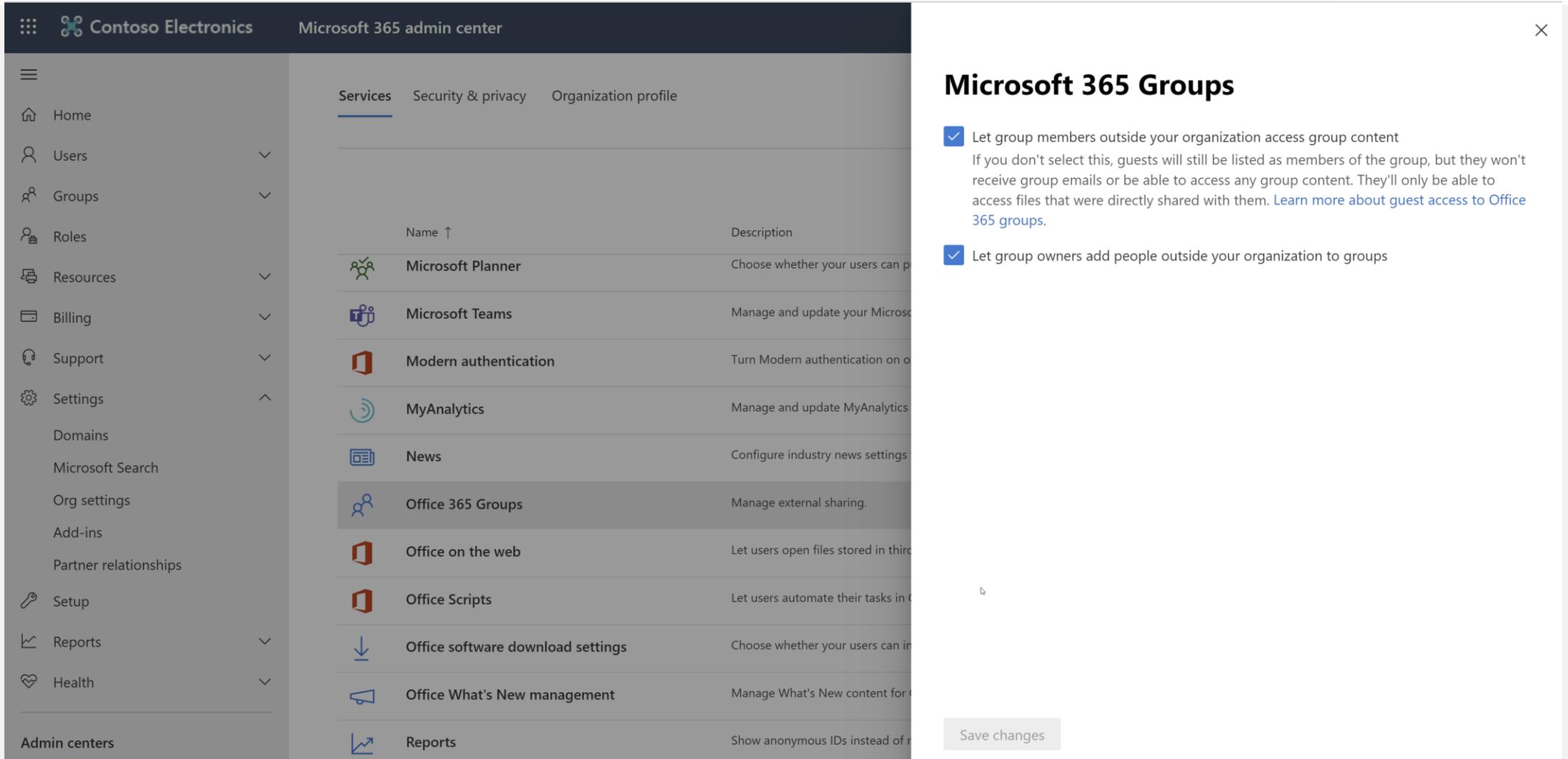
You can also [change the external sharing settings for SharePoint.](#)

Let users add new guests to the organization

Save changes



O365 Groups: Owners can *add* guests?



The screenshot shows the Microsoft 365 admin center interface for 'Contoso Electronics'. The left sidebar contains navigation options: Home, Users, Groups, Roles, Resources, Billing, Support, Settings, Domains, Microsoft Search, Org settings, Add-ins, Partner relationships, Setup, Reports, and Health. The main content area is titled 'Microsoft 365 admin center' and has tabs for 'Services', 'Security & privacy', and 'Organization profile'. The 'Services' tab is active, displaying a list of services. The 'Office 365 Groups' service is highlighted, showing a description: 'Manage external sharing.' To the right, a settings panel titled 'Microsoft 365 Groups' is open, showing two checked options: 'Let group members outside your organization access group content' and 'Let group owners add people outside your organization to groups'. A 'Save changes' button is visible at the bottom of the settings panel.

Name ↑	Description
Microsoft Planner	Choose whether your users can p
Microsoft Teams	Manage and update your Microsc
Modern authentication	Turn Modern authentication on o
MyAnalytics	Manage and update MyAnalytics
News	Configure industry news settings
Office 365 Groups	Manage external sharing.
Office on the web	Let users open files stored in thir
Office Scripts	Let users automate their tasks in C
Office software download settings	Choose whether your users can in
Office What's New management	Manage What's New content for c
Reports	Show anonymous IDs instead of r

Microsoft 365 Groups

- Let group members outside your organization 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. [Learn more about guest access to Office 365 groups.](#)
- Let group owners add people outside your organization to groups

Save changes



Microsoft Teams: Are guests allowed in Teams?

The screenshot shows the Microsoft Teams admin center interface for Contoso Electronics. The left-hand navigation pane includes options like Dashboard, Teams, Devices, Locations, Users, Meetings, Messaging policies, Teams apps, Voice, Policy packages, Analytics & reports, and Org-wide settings. The 'Guest access' option is highlighted. The main content area is titled 'Guest access' and contains the following settings:

- Allow guest access in Teams:** A toggle switch is turned 'On'.
- Calling:** A section header for managing calling controls for guest users.
- Make private calls:** A toggle switch is turned 'On'.
- Meeting:** A section header for settings for guests in meetings.
- Allow IP video:** A toggle switch is turned 'On'.
- Screen sharing mode:** A dropdown menu is set to 'Entire screen'.

If "YES", owner invitation of new guests dictated by Office 365 Groups setting



Going Further – Microsoft *Information Barriers*

Leveraging our *AAD properties* and segments to create hard divisions that block sharing and communications *within a tenant*.

This group...	...can't talk to this group...	...because...
Investment Banking	Research	FINRA Regulations
Lawyer for Client A	Lawyer for Client B	Conflict of interest within a firm
Professional Services	Off-shore Development	Government contracts
US Weapons Developers	Overseas Subsidiaries	ITAR Compliance



Jefferies



Customer:
Jefferies

Industry:
Banking & Capital Markets

Size:
3,900 employees

Country:
United States

Products and services:
Microsoft 365
Microsoft Teams
Microsoft OneDrive

Microsoft SharePoint
Microsoft 365 Information Barriers
Microsoft 365 Multi-Geo

Microsoft Information Protection

Microsoft Defender Antivirus

[Read full story here](#)

“We were pleased that the information barriers feature was already ‘baked in’ to Microsoft 365. By implementing information barriers we were able to successfully deploy Teams, OneDrive, and SharePoint Online.”

—Jitesh Mandalia, Senior Vice President, Jefferies

Situation:

The global, independent investment banking, capital markets and alternative asset management firm Jefferies wanted its employees to collaborate using Microsoft Teams, OneDrive, and SharePoint. It needed to be sure it complied with banking and investment regulations.

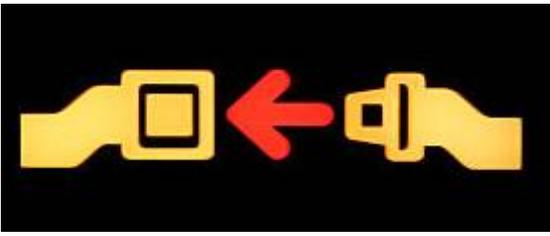
Solution:

The company adopted information barriers, which is included in its Microsoft 365 E5 license, and was able to establish barriers between its investment banking and research divisions. Users across those divisions cannot digitally see or contact each other.

Impact:

In deploying information barriers, Jefferies could quickly get employees collaborating using Teams, OneDrive, and SharePoint. Even while transitioning to the cloud-based platform while 98 percent of the company worked remotely, it had a successful quarter.





Getting started with Information Barriers

- Step 1 – Review Prerequisites (Licensing, AAD Attributes, Teams Name Search Enabled, Audit On, Admin Consent)
- Step 2 – Segment Users
- Step 3 – Create Barriers
- Step 4 – Apply Barriers
- Step 5 – Configure for SPO & OD4B

E5 License Required



Create Segment using AAD Attributes

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](#)

[Next](#) [Close](#)

[What's new?](#) [+ Add cards](#)

Communication compliance

Minimize communication risks

Quickly setup policies to monitor user communications across channels for inappropriate and sensitive content so they can be examined by designated reviewers. [Learn more about communication compliance](#)

Recently detected

Communications containing	Instances
U.S. Driver's License Nu...	181
New Zealand Social Wel...	9
New Zealand Inland Rev...	6

Discover Shadow IT

Data isn't available right now

Active alerts

0 active alert



Creating Policy

Contoso Electronics Microsoft Purview

Information barrier > Policies > Create policy

Name

Assigned segment

Communication and collaboration

Policy status

Review your settings

Provide a policy name

Name *

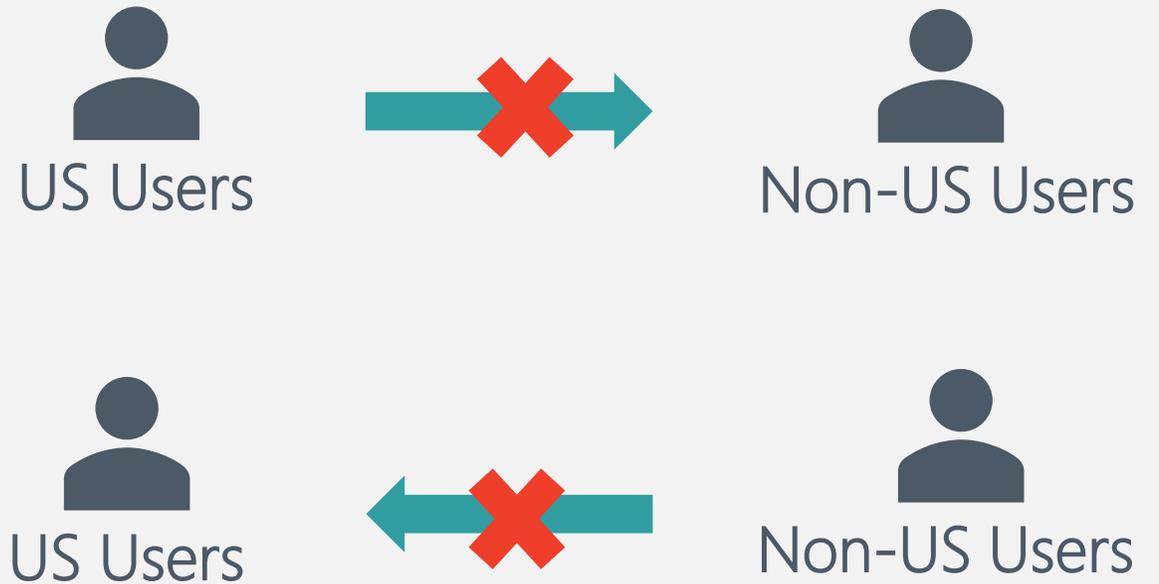
Next Cancel



Don't Forget Communication is two ways!



You will need to create two policies



Going Further – Microsoft *Information Barriers*

Leveraging our *AAD properties* and segments to create hard divisions that block sharing and communications *within a tenant*.

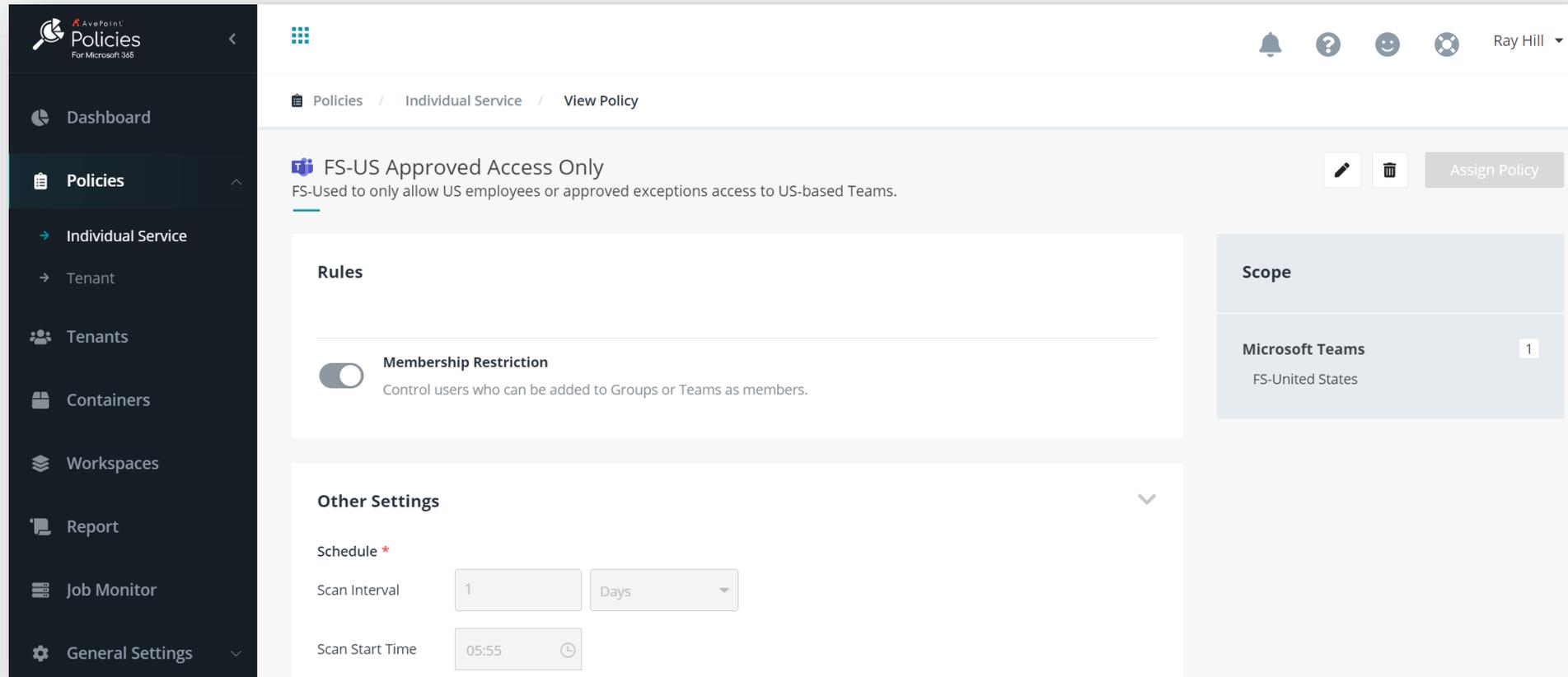
This group...	...can't talk to this group...	...because...
Investment Banking	Research	FINRA Regulations
Lawyer for Client A	Lawyer for Client B	Conflict of interest within a firm
Professional Services	Off-shore Development	Government contracts
US Weapons Developers	Overseas Subsidiaries	ITAR Compliance

But... what if this isn't *always* true in a shared tenant?



Right-sizing Governance – *AvePoint Policies*

For the *sometimes* scenarios – let's combine the AAD classifications with our Teams and Groups Memberships!



The screenshot displays the AvePoint Policies management console. On the left is a dark navigation sidebar with options: Dashboard, Policies (selected), Individual Service, Tenant, Tenants, Containers, Workspaces, Report, Job Monitor, and General Settings. The main content area shows the 'View Policy' page for 'FS-US Approved Access Only'. The breadcrumb trail is 'Policies / Individual Service / View Policy'. The policy description is 'FS-Used to only allow US employees or approved exceptions access to US-based Teams.' Action buttons for edit, delete, and 'Assign Policy' are visible. The 'Rules' section has a 'Membership Restriction' toggle that is turned on, with the description 'Control users who can be added to Groups or Teams as members.' The 'Other Settings' section includes a 'Schedule' field with a 'Scan Interval' of 1 Days and a 'Scan Start Time' of 05:55. On the right, the 'Scope' section shows 'Microsoft Teams' with 'FS-United States' and a count of 1.





FS-US Approved Access Only

FS-Used to only allow US employees or approved exceptions access to US-based Teams.



Assign Policy

Rules



Membership Restriction

Control users who can be added to Groups or Teams as members.

Scope

Microsoft Teams

FS-United States

1

Other Settings

Schedule *

Scan Interval

1

Days

Scan Start Time

05:55



Dashboard

Policies

Individual Service

Tenant

Tenants

Containers

Workspaces

Report

Job Monitor

General Settings





 Dashboard

 Policies 

 Individual Service

 Tenant

 Tenants

 Containers

 Workspaces

 Report

 Job Monitor

 General Settings 

Name *

FS-US Approved Access Only

Description

FS-Used to only allow US employees or approved exceptions access to US-based Teams.

Rules





Membership Restriction

Control users who can be added to Groups or Teams as members.





Polices / Individual Service / Edit Policy

Name *
FS-US Approved Access Only

Description
FS-Used to only allow US employees or approved exceptions access to US-based Teams.

Rules

Membership Restriction
Control users who can be added to Groups or Teams as members.

Other Settings

Schedule *

Scan Interval: 1 Days

Scan Start Time: 05:55

Retention Duration *

Membership Restriction

Control users who can be added to Groups or Teams as members.

Add a filter to this rule

Crisis Management

[View Details](#)

Rule Settings

Choose who can be added to Groups or Teams as members: *

Only allow the specified users to be added to Groups or Teams as members

Select a Defined Group

FS-United States

[View Details](#)

Restrict the specified users from being added to Groups or Teams as members

If violations are identified, take the following action:

Remove the out-of-policy users

Send e-mail notifications of the violations to the following users:

Include Group/Team owners

Include primary/secondary contacts configured in Cloud Governance

Cancel OK



Right-Sizing Governance Controls

Control users who can be added to Groups or Teams as members.

Add a filter to this rule 

Crisis Management

[View Details](#)

Filter Conditions *

Group Team Site Property

Custom Property: CrisisCritical Equals Yes

And

Custom Property: Region Equals North America

Choose who can be added to Groups or Teams as members: *

Only allow the specified users to be added to Groups or Teams as members

Select a Defined Group

FS-United States

[View Details](#)

Restrict the specified users from being added to Groups or Teams as members

Meet [All](#) of the following conditions

Conditions

User Property

Custom AAD Attribute: Country or region Equals United States

Display Name Equals ATSAAdmin

Display Name Equals Lucia Micarelli



Right-Sizing Governance Controls

If violations are identified, take the following action:

- Remove the out-of-policy users

Send e-mail notifications of the violations to the following users:

- Include Group/Team owners
- Include primary/secondary contacts configured in Cloud Governance



Building Blocks for Microsoft Policies

Add Rule to Microsoft Teams

Select a rule to add to the policy:

Select One

Classification Enforcement



External Sharing Settings



External User Access Enforcement



Groups/Teams Creation Restriction



Membership Restriction



Select a rule to add to the policy.





**Where are
we now?**

- ~~Securing *Identity*~~
- Securing *Data*
- Securing *Workspaces*
- Putting it all together...



**YOU
ARE
HERE**



Where does this conversation fit in...

IT Governance

(Broad, organization-wide)

Application Governance

(Application-specific, aligns with IT Governance goals)

SharePoint

OneDrive

Office 365

Other Applications

Data Governance

(Content-specific, aligns with IT Governance goals)

Retention/Expiration

Records Mgmt

Classification

Data Protection

"ADG"

"AIP"

FOCUS



Out-of-box sensitive info types

Microsoft 365 includes hundreds of sensitive info types

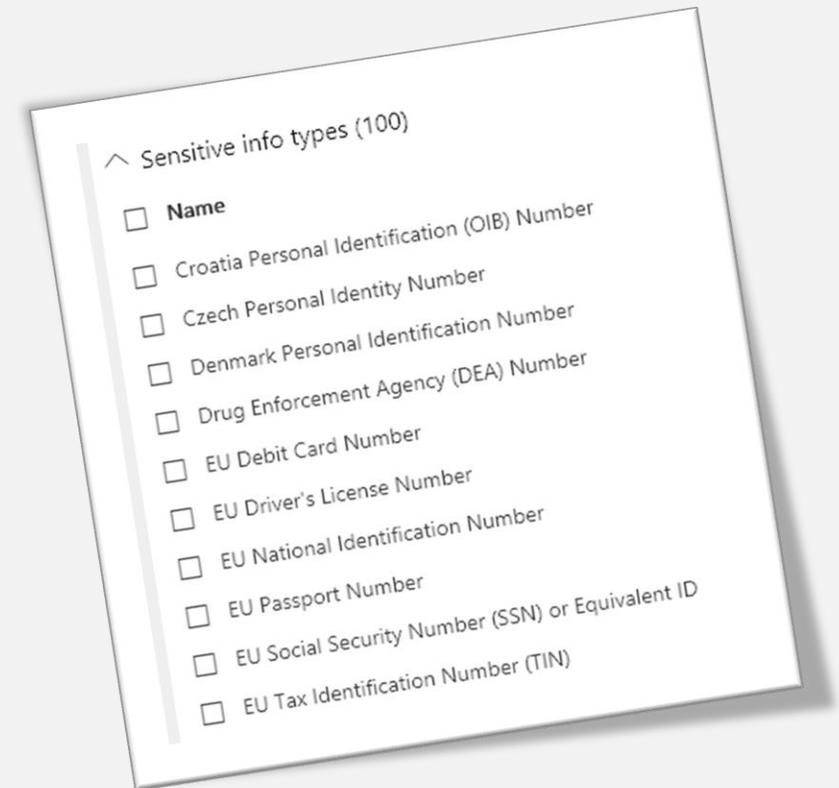
For different countries, industries or by information type

Sensitive information comes in many forms

Financial data, Personally Identifiable Information (PII)

Examples

- Croatia Personal Identification (OIB) Number
- EU Debit Card Number
- EU Passport Number
- US Drivers License Number
- Social Security Number



E3 License Required

Customer specific sensitive info types

Business intellectual property

Business plans, product designs, confidential projects

Employee or customer information

HR Information, resumés, employment records, salary information

Highly confidential information

Mergers and Acquisition, workforce reduction

Examples

- Employee or customer numbers *Technology: RegEx*
 - <EMP-nnnnn>
 - <CUST-nnnnnn-NL>
- Specific keywords *Technology: Static Keywords*
 - <Project Enigma>
 - <Highly Confidential>
 - <Internal only>



- Home
- Compliance Manager
- Data classification**
- Data connectors
- Alerts
- Reports
- Policies
- Permissions

Data classification

Overview Trainable classifiers Sensitive info types Exact data matches Content explorer

Get snapshots of how sensitive info and labels are being used across your organization's locations. [Learn more](#)

Top sensitive info types

Sensitive info types used most in your content



Finding sensitive information in M365 (E3)

DLP Policy Rule One

Name Conditions Exceptions Actions User notifications User overrides Incident reports Options

We'll apply this policy to content that matches these conditions.

Content contains

Any of these ▾

Sensitive info type	Instance count		Match accuracy		
	min	max	min	max	
U.S. Bank Account Number	1	any	75	100	×
U.S. Driver's License Number	1	any	75	100	×
U.S. Individual Taxpayer Identification Number (ITIN)	1	any	75	100	×
U.S. Social Security Number (SSN)	1	any	75	100	×

Add ▾

+ Add group

Content is shared

only with people inside my organization ▾

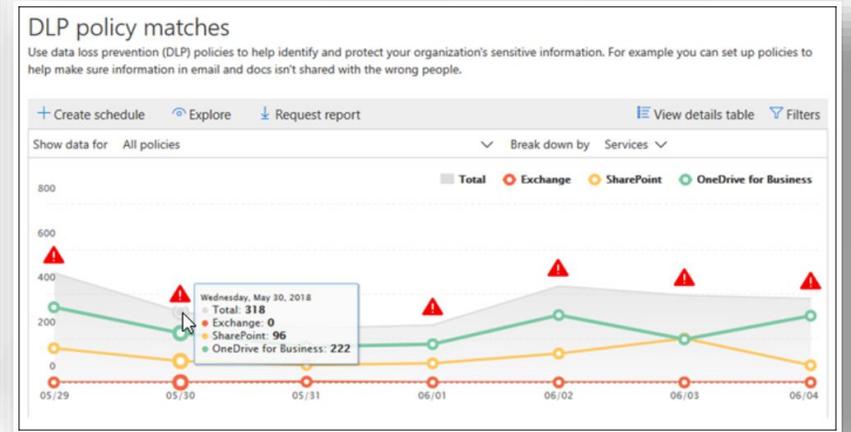
only with people inside my organization

with people outside my organization

+ Add a condition ▾

Notifications for internal or external sharing.

DLP Policies allow for notifications, as well as visibility into where sensitive content exists.



Create DLP Rules to Restrict Access or Encrypt

Edit rule

Restrict access or encrypt the content in Microsoft 365 locations

Restrict access or encrypt the content in Microsoft 365 locations

- Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files.
By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams.
- Block everyone. [i](#)
- Block only people outside your organization. [i](#)

Take Action

+ Add an action

User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

On

[i](#) Support and behavior for policy tips varies across apps and platforms. [Learn where policy tips are supported](#)

Microsoft 365 services

Notify users in Office 365 service with a policy tip

Email notifications

- Notify the user who sent, shared, or last modified the content.
- Notify these people:
- The person who sent, shared, or modified the content
 - Owner of the SharePoint site or OneDrive account

Notifications for end users can be customized with Tips

E5 License Required

Microsoft Information Protection

Protect your sensitive data – wherever it lives or travels



Discover



Classify



Protect



Monitor

Across



Devices



Apps



Cloud services



On-premises



SENSITIVITY LABELS PERSIST WITH THE DOCUMENT

Document labeling – what is it?

Metadata written into document files

Travels with the document as it moves

In clear text so that other systems can read it

Can be used to apply a protection action or data governance action

Can be customized per the organization's needs



Creating "Sensitivity Labels" in the S&C Center

Contoso Electronics Microsoft 365 compliance

Information protection Remove from navigation

Labels Label policies Auto-labeling

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label Publish label Refresh 6 items

Name	Order	Scope	Created by	Last modified
Personal	0 - lowest	File,Email	Johanna Lorenz	Jul 19, 2021 6:52:47...
Public	1	File,Email	Johanna Lorenz	Jul 19, 2021 6:52:48...
General	2	File,Email	Johanna Lorenz	Jul 19, 2021 6:52:48...
> Confidential	3	File,Email	Johanna Lorenz	Jul 19, 2021 6:52:49...
∨ Highly Confidential	7	File,Email	Johanna Lorenz	Jul 19, 2021 7:08:05...
Recipients Only	8	File,Email	Johanna Lorenz	Jul 19, 2021 6:52:56...
All Employees	9	File,Email	Johanna Lorenz	Jul 19, 2021 7:08:06...
Anyone (not protected)	10	File,Email	Johanna Lorenz	Jul 19, 2021 6:52:58...
Project Obsidian	11	File,Email,Site,UnifiedGroup	Johanna Lorenz	Jul 19, 2021 7:08:07...



Building Your Sensitivity Labels

New sensitivity label

- ✓ Name & description
- ✓ Scope
- ✓ Files & emails
- ✓ Groups & sites
- ✓ Azure Purview assets (preview)
- Finish

Review your settings and finish

Name

Test Label

[Edit](#)

Display name

My Test Label

[Edit](#)

Description for users

Test

[Edit](#)

Scope

File,Email,Site,UnifiedGroup,PurviewAssets

[Edit](#)

Encryption

Encryption

[Edit](#)

Content marking

Watermark: RESTRICTED

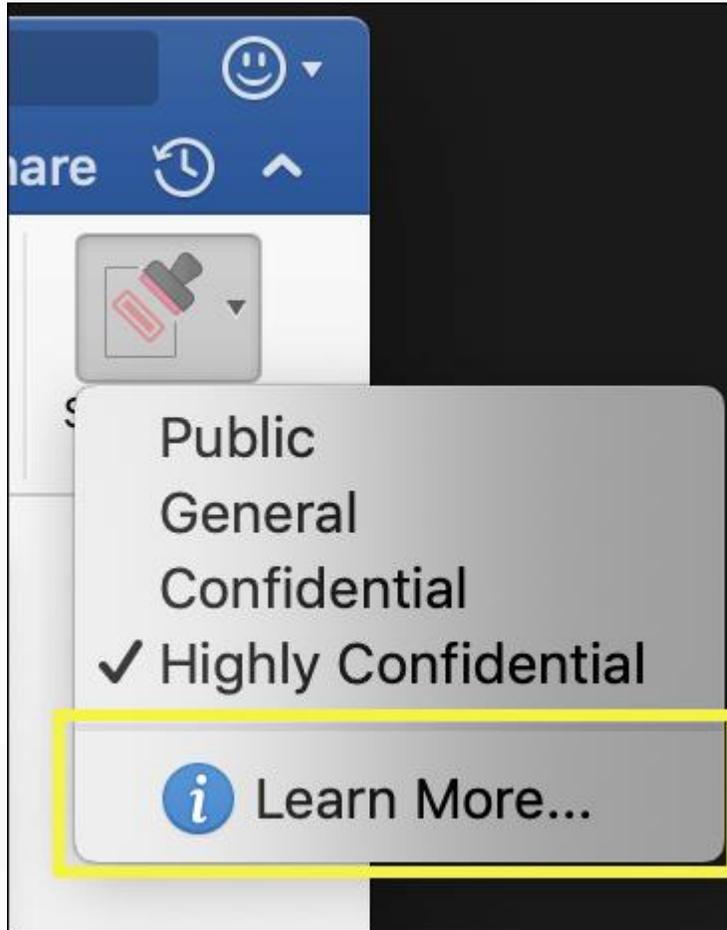
[Back](#)

[Create label](#)

[Cancel](#)



Getting Labels on Content – Auto vs Manual Labeling



Manual Labeling

Requires Some user training

No data map or trainable classifiers needed

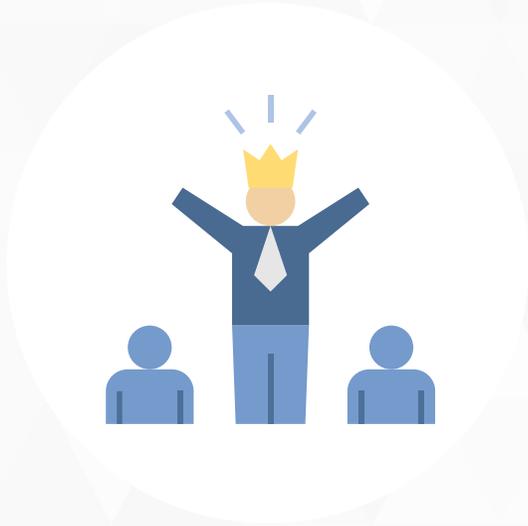
Encrypt Items

Content Marking

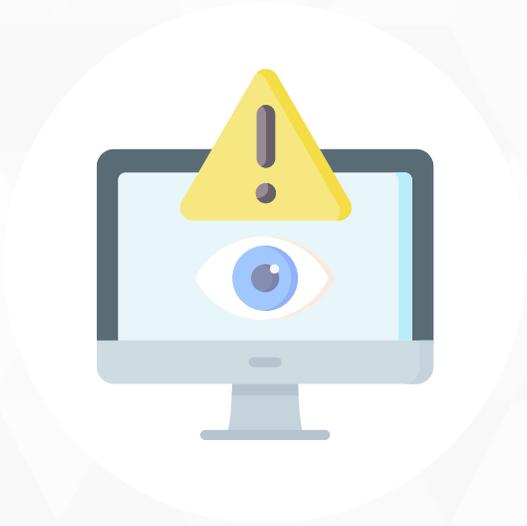
Time-bomb Files (up to 100 days)



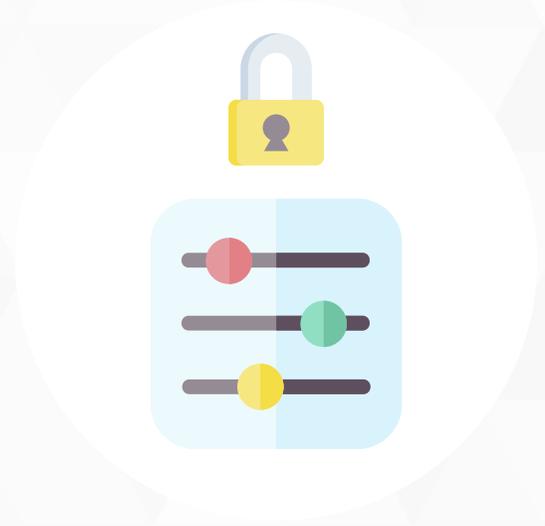
Sensitive data in a “free and open sharing” system?



Office 365 gives “Owners” significant privilege



Anyone can be an owner, but even members can share content



THE ANSWER: Right-sizing control based on risk

Understanding the impact of Public/Private for Groups and Teams...

The image shows a Microsoft Teams interface. At the top, there's a "Join or create a team" header. Below it, there are options to "Create a team" with three circular icons. A card for "Software Development" is visible, showing "2 members | Public".

A dialog box titled "What kind of team will this be?" is open, showing two options: "Private" (with a lock icon) and "Public" (with a globe icon). The "Public" option is selected and highlighted with a mouse cursor.

Below the dialog, the "My Public Team" page is shown. The team name "My Public Team" is displayed with a red box around the "Public group" label. A red arrow points from this label to the "Permissions" panel on the right.

The "Permissions" panel is open, showing a list of permissions. The "Site members" section is expanded, and the "Ee" permission (Everyone except external users) is highlighted with a red box. Other permissions include "Site owners", "Site visitors", and "Site sharing".

At the bottom of the page, there is a footer: "©AvePoint, Inc. All rights reserved. Confidential".

Understanding the default sharing options for all SharePoint sites...

Site sharing settings

Control how things in this site can be shared and how request access works.

Sharing permissions

- Site owners and members can share files, folders, and the site. People with Edit permissions can share files and folders.
- Site owners and members, and people with Edit permissions can share files and folders, but only site owners can share the site.
- Only site owners can share files, folders, and the site.

Access requests

Allow access requests

Choose who will receive requests for this site:

- BGLeads Owners
- Specific email addresses

Add a custom message to the request page:

For example: Please review your request.

Save

Word ABC Co SOW - Saved

File Home Insert Layout References Review View Help Table Editing

Share

Link settings

Who would you like this link to work for? [Learn more](#)

- Anyone with the link
- People in AvePoint ATS Dev with the link
- People with existing access
- Specific people

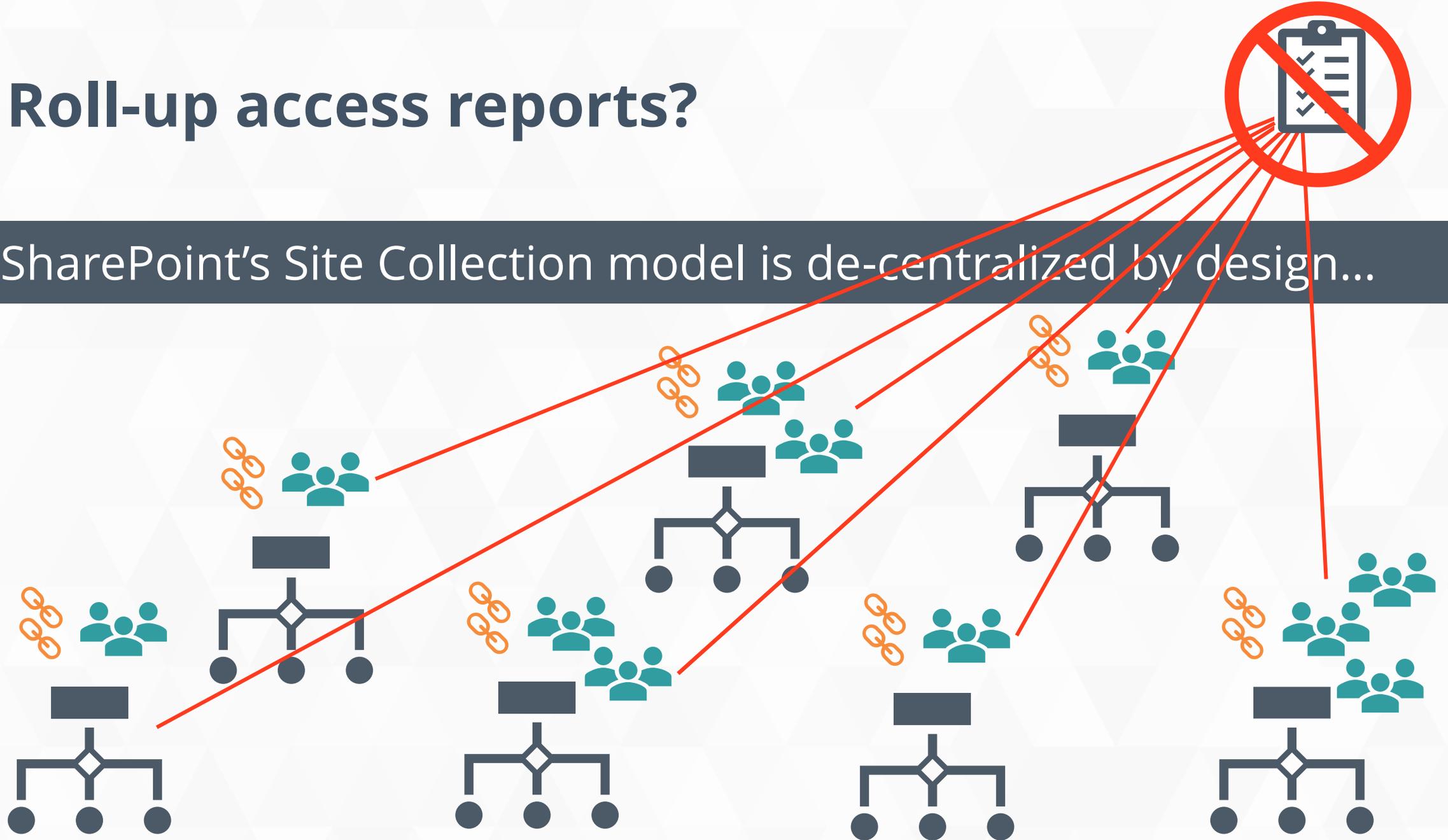
Other settings

- Allow editing
- Open in review mode only
- Block download

Apply Cancel

Roll-up access reports?

SharePoint's Site Collection model is de-centralized by design...



How do you manage security settings?



M365 Access Reviews and Admin Settings don't tell the whole story.



Marco still does not have a top-down view.

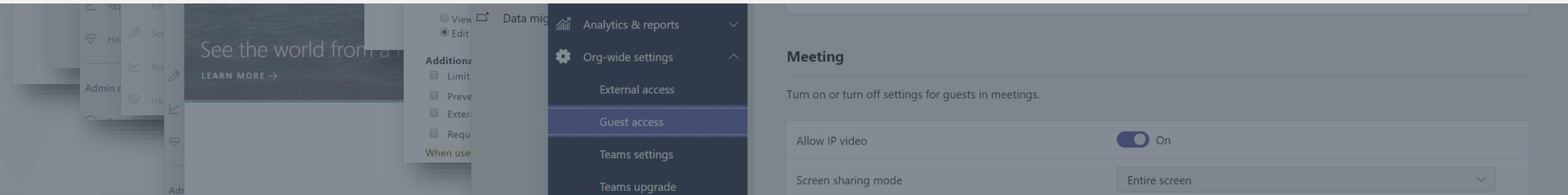


He can't identify who has access to what information.



Not enough context to tailor policies for audiences and purpose.

Marco is exhausted.





Policies & Insights



Microsoft / Office 365

With PI, organizations can unleash user adoption and the power of Microsoft 365 sensitive information types and security controls, without becoming a security expert. PI guides admins towards appropriate controls with prioritized insights. Set robust controls from one place, that get enforced automatically.



TAP INTO VALUABLE M365 DATA TO PRIORITIZE INSIGHTS

We aggregate sensitive information types and data from Microsoft's own activity feed to keep you focused on what matters



PUT MICROSOFT SECURITY CONTROLS TO WORK

With central access to critical configurations for guest access, sharing, and more - we make it easy to get the control you need

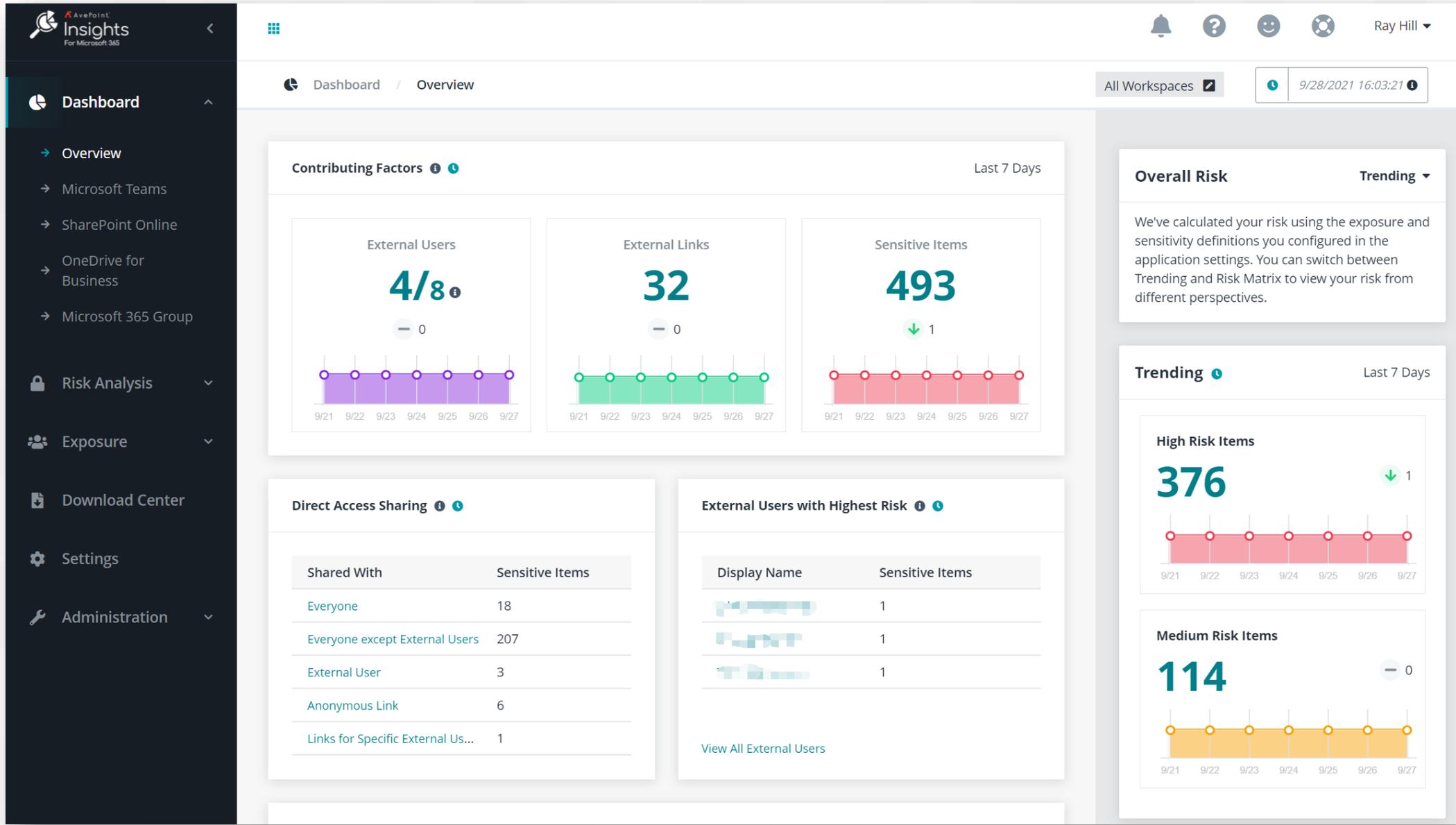


REDUCE IT WORKLOAD FOR ONGOING MANAGEMENT

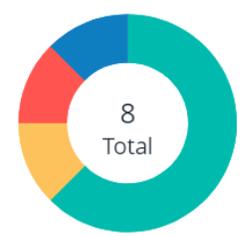
Prevent configuration drift with policies that get enforced automatically. We enable control, without impeding user adoption



Drawing Your Attention to *Higher Levels*

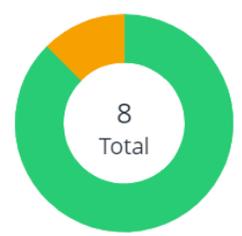


Domains ▾ with Most External Users ℹ 🔔



Domain Name	External Users
gmail.com	5
avepoint.com	1
avepointats-d...	1
live.com	1

Status 🔔



Status	External User Count
Active	7
Orphaned ℹ	1
Blocked	0
Not in AAD	1

Export 🔍 🗑️ 🎯 🚫 🔄

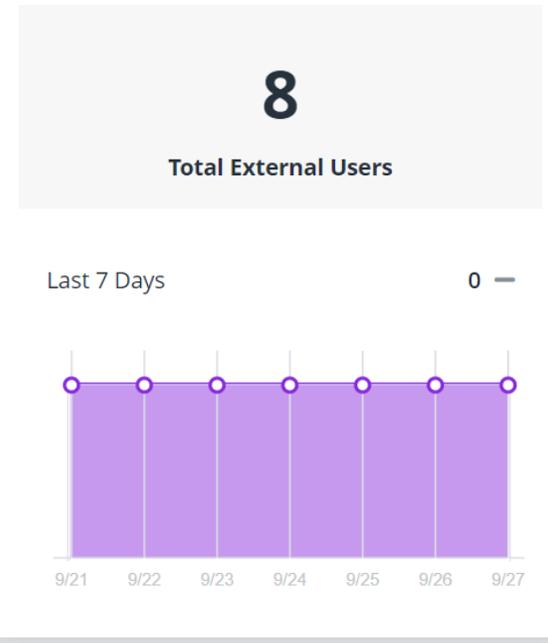
<input type="checkbox"/>	Display Name ▾	Email	Sensitive Items ℹ 🔔 ▾	Last Sign-in 🔔	Time
<input type="checkbox"/>	...	✖ [Redacted]	1	▲ N/A	
<input type="checkbox"/>	...	🎯 [Redacted] Trusted	1	▲ None	
<input type="checkbox"/>	...	🎯 [Redacted]	1	▲ None	
<input type="checkbox"/>	...	🎯 [Redacted]	0	▲ 28 Days	
<input type="checkbox"/>	...	🎯 [Redacted] Trusted	0	▲ None	
<input type="checkbox"/>	...	🎯 [Redacted] Trusted	0	▲ 7 Days	

External user statistics have ... ▾

Limiting external user access in your environment means reducing the risk of sensitive information leaving your organization!

External User Trend 🔔

This section shows the external user statistics of the selected workspace in the last 7 days.



User-Level Insights Across our Tenants

Exposure / External Users / Access Report

Last Aggregated Time 10/5/2022 06:20:30

Murugan Balaji

Export

Known Risk (Direct) Possible Risk (Indirect)

By Site By Object

This table shows the site collections to which the user has been given direct access or where permissions are inherited from SharePoint groups. These are permissions you can control. You can click anywhere in a site collection row to drill down and view more details.

Site Name	Workspace	Object Type	Created By	External Sharir
2019 Marketing Wei Office			2023 marketing Owners	New and existir
2019 Marketing Wei Office			MarketC Owners	New and existir
2019 Marketing Wei Office			marketd Owners	New and existir
2019 Marketing Wei Office			Tom Gawczynski	Existing guests
2022MarketingWeiOffice			2022MarketingWeiOffice Owners	New and existir
Accounting NA			Hunter Willis	Anyone
Department of Defense			Tom Gawczynski	Anyone

Murugan Balaji

Risk Overview

Known Risk
This section shows the total number of sensitive items this user has direct access to by name.

High 1 Medium 86 Low 0

Total Sensitive Items 87

Possible Risk
This section shows the total number of security groups from which the user inherits permissions to objects.

Total Groups 3

User Activities

Used secure link OVER A MONTH AGO

Accessed file OVER A MONTH AGO
Accessed from "Documents"

Customer success: City of Port St. Lucie

“

When we first ran Policies and Insights, it came up with thousands of links that were shared incorrectly. We hit a button and it basically fixed all the links and that risk was instantly mitigated.

Hannah Melton, Assistant Director IT



ENABLE REMOTE WORK IN COVID-19 RESPONSE

Migrated to Microsoft 365 with AvePoint within 12 hours. Leveraging AvePoint's governance, security, and backup solutions, was able to drive adoption and minimize risk.



COMPLY WITH LOCAL REGULATIONS

Monitor access to sensitive documents, automatically remediate policy violations for guest access. Security dashboards provide actionable insights. Paired with AvePoint's granular backup and restore, meet "Sunshine State" protection laws.



REDUCE MANUAL IT WORK TO ROLL-OUT & MANAGE TEAMS

Reduce Teams provisioning process by 600%, automatically fix links that are shared incorrectly, and prevent configuration drift with governance + PI capabilities. No more manual configuration and membership checks to validate access!





Where are
we now?

- ~~Securing *Identity*~~
- ~~Securing *Data*~~
- Securing *Workspaces*
- Putting it all together...



YOU
ARE
HERE



Top-down, and bottom-up...

You can't chase every document!

"Container level"

"Content level"

Operational Governance
(Application-specific, aligns with IT Governance goals)

Data Governance
(Content-specific, aligns with IT Governance goals)

Workspace Provisioning

Ongoing Management & Enforcement

Lifecycle and EOL for Workspaces

Item-level Retention & Expiration

Records Mgmt

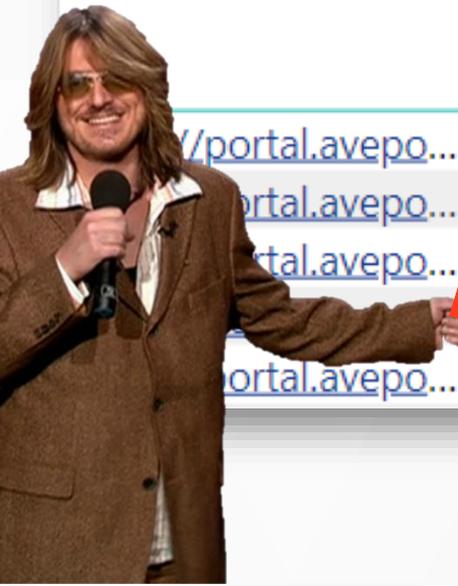
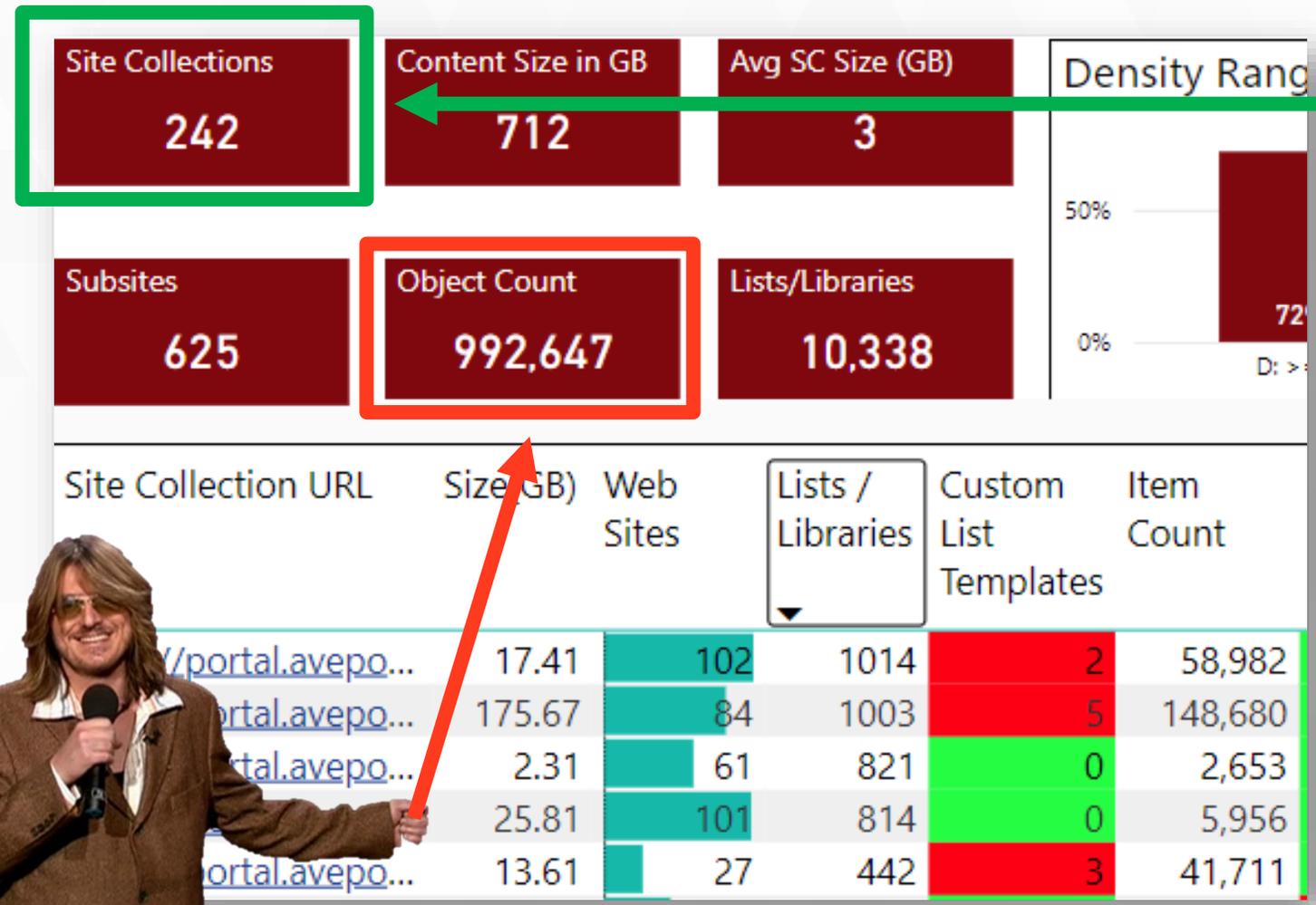
Classification

DLP



Container Level Labeling is Obtainable!

Labeling at a Site/Group/Team require a lot less effort than looking into a millions of individual files. This can help establish baseline internal & external rules around sharing and access especially when paired with conditional access.



Create Labels and Select Groups & Sites

Define the scope for this label

Labels can be applied directly to files, emails, containers like SharePoint sites and Teams, Power BI items, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. [Learn more about label scopes](#)



Items

Configure protection settings for labeled emails, Office files, and Power BI items. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.



Groups & sites

Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.



Schematized data assets (preview)

Apply labels to files and schematized data assets in Microsoft Purview Data Map. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

Important

Only these site and group settings take effect when you apply the label to a team, group, or site. If the **label's scope** includes files and emails, other label settings such as encryption and content marking aren't applied to the content within the team, group, or site.



Sensitivity Labels for teams, groups and sites

Creating the Sensitivity Labels in Security and Compliance Center

Office 365 Security & Compliance

Edit sensitivity label

- ✓ Name & description
- ✓ Encryption
- ✓ Content marking
- ✓ Endpoint data loss prevention
- Site and group settings
- Auto-labeling for Office apps
- Review your settings

Site and group settings

Select the settings you want to take effect when this label is applied to an Office 365 group or SharePoint site. Note that the settings aren't applied to files, so they don't impact downloaded copies of files. [Learn more about site and group protection](#)

Site and group settings

Privacy of Office 365 group-connected team sites

Private - only members can access the site

External users access

Let Office 365 group owners add people outside the organization to this site

Unmanaged devices

Allow full access from desktop apps, mobile apps, and the web

Allow limited, web only access

Block access

What kind of team will this be?

Sensitivity [Learn more](#)

Internal Workspace

Teams with this sensitivity must be private.

Private
People need permission to join

Public
Anyone in your org can join

Org-wide
Everyone in your organization automatically joins

< Back

Team creation wizard

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide#using-sensitivity-labels-for-microsoft-teams-microsoft-365-groups-and-sharepoint-sites>

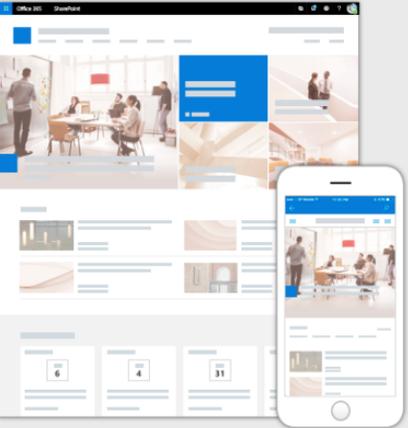
SharePoint & Group Sites Experience

Communication Site

Choose a design

Topic

Use this design if you have a lot of information to share such as news, events, and other content.



Site name

Site owner

Enter a name or email address

Select a language

English

Select the default site language for your site. You can't change this later.

Advanced settings ^

Sensitivity

Confidential \ All Employees

Time zone

(UTC-08:00) Pacific Time (US and Canada)

Site description

Tell people the purpose of this site

Storage limit

25600 GB

Finish Cancel

SharePoint

Your organization doesn't allow you to download, print, or sync using this device. To use these actions, use a device that's joined to a domain or marked compliant by Intune.

SP Solar Panels GenY
Private group | Confidential

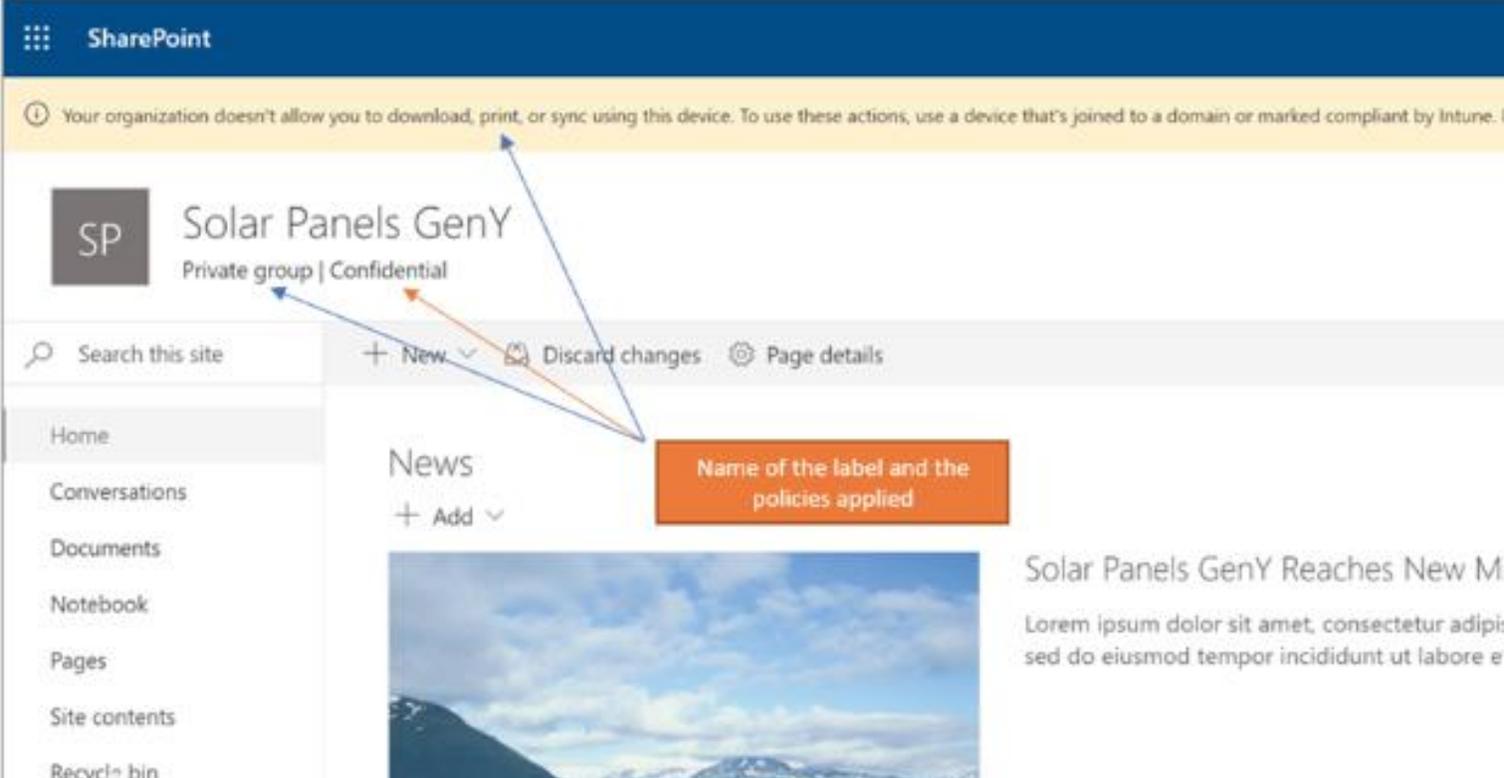
Search this site + New Discard changes Page details

Home
Conversations
Documents
Notebook
Pages
Site contents
Recycle bin

News + Add

Name of the label and the policies applied

Solar Panels GenY Reaches New M
Lorem ipsum dolor sit amet, consectetur adipi
sed do eiusmod tempor incididunt ut labore e



Putting it all together!



Establishing data ownership

Workspace level classification

Collaboration asset inventory

Attestation/Recertification

Automated self-service requests

End-to-end lifecycle management



What is sprawl?



Not a number...

... just more than you can effectively manage

Cutting through the noise...

*Maintaining an
inventory of your
collaborative
workspaces*



Admins have an "inventory" of all M365 collaborative workspaces

Workspace report

Search in Workspace report | Export report | Mail all contacts | Refresh | 0 workspaces selected

Phase	Name	Status	Type	URL	Policy	Data owners	Classification	Critical Business
Compliance status: Renewal pending	R&D Team Site	Deleted	Site Collection	https://avepointasd...	SC Intranet Policy	Barriemore Barlow Ian Anderson Ray Hill	-	-
	Quarterly Conference	Archived	Microsoft Team	https://avepointasd...	Internal Group Team...	Barriemore Barlow Barriemore Barlow Ian Anderson	-	No
	Q2 Outing	Active	Microsoft Team	https://avepointasd...	Guest Group Team P...	Barriemore Barlow; R... Ray Hill Ian Anderson	-	No
	publictoprivate	Active	Microsoft Team	https://avepointasd...	-	Barriemore Barlow - -	-	-
	Public-Team_EIPaso	Deleted	Microsoft Team	https://avepointasd...	Private Team Policy	Ray Hill; Ian Anderson Ray Hill Ian Anderson	-	-
	Public-ShoeDeal	Deleted	Microsoft Team	https://avepointasd...	Private Team Policy	Ray Hill Ray Hill Ian Anderson	-	-
	Public-SalesWestVAT	Deleted	Microsoft Team	https://avepointasd...	Private Team Policy	Ray Hill Barriemore Barlow Ray Hill	-	-
	PublicProductXYZ	Deleted	Microsoft Team	https://avepointasd...	Public Short Term Te...	Ray Hill Ray Hill Ian Anderson	-	-
	Public-PDT	Deleted	Microsoft 365 Group	https://avepointasd...	Private Team Policy	Ian Anderson Ian Anderson Ray Hill	-	No
	Public-New Marketing	Deleted	Microsoft Team	https://avepointasd...	Public Short Term Te...	Ian Anderson - Ray Hill	-	-
	PublicMarketingEvents	Deleted	Microsoft Team	https://avepointasd...	Public Short Term Te...	Ray Hill Ray Hill Ian Anderson	-	-
	Public-internal_project	Deleted	Microsoft 365 Group	https://avepointasd...	Private Team Policy	Ray Hill Barriemore Barlow Ian Anderson	-	No
	Public-internal_Project	Deleted	Microsoft Team	https://avepointasd...	Private Team Policy	Ray Hill Ray Hill Ian Anderson	-	-
	Public-Internal HR Proj	Deleted	Microsoft Team	https://avepointasd...	Public Team Policy	Ray Hill Ray Hill Ian Anderson	-	-
	PublicHRUpdates	Deleted	Microsoft Team	https://avepointasd...	Public Team Policy	Ray Hill Ray Hill Ian Anderson	-	-
	PublicHRCommunicati	Deleted	Microsoft Team	https://avepointasd...	Public Team Policy	Ray Hill Ray Hill Ian Anderson	-	-
	PublicGroupe-Exemple	Deleted	Microsoft 365 Group	https://avepointasd...	Public Team Policy	Barriemore Barlow \$requester \$managerofrequester	-	-

Admins have deep visibility into all built-in and organizational metadata

The screenshot displays the AvePoint Cloud Governance interface. At the top, there's a navigation bar with the AvePoint logo and 'Cloud Governance' text. Below it, a search bar and action buttons like 'Export report', 'Mail all contacts', and 'Refresh' are visible. A left-hand navigation pane includes sections for 'Home', 'Management', 'Services', 'Profiles', 'Service templates', 'Settings', 'MyHub settings', 'System settings', 'Directory', 'Workspace report', and 'Job monitor'. The main area shows a 'Workspace report' table with columns: Phase, Name, Status, Type, URL, Policy, Primary admin, Primary Data Ow..., and Secondary contact. A red arrow points from the text 'Any additional Metadata' to the 'Additional Information' section of the 'Choose columns (14)' dialog box. This dialog box lists various metadata fields with checkboxes, including 'Classification' and 'Critical Business Application' which are checked.

Phase	Name	Status	Type	URL	Policy	Primary admin	Primary Data Ow...	Secondary contact
✓	R&D Team Site	Deleted	Site Collection	https://avepointatsd...	SC Intranet Policy	Barriemore Barlow	Ian Anderson	Ray Hill
✓	Quarterly Conference	Archived	Microsoft Team	https://avepointatsd...	Internal Group Team...	Barriemore Barlow	Barriemore Barlow	Ian Anderson
🕒	Q2 Outing	Active	Microsoft Team	https://avepointatsd...	Guest Group Team P...	Barriemore Barlow, R...	Ray Hill	Ian Anderson
🕒	publictoprivate	Active	Microsoft Team	https://avepointatsd...	-	Barriemore Barlow	-	-
✓	Public-Team_EIPaso	Deleted	Microsoft Team	https://avepointatsd...	Private Team Policy	Ray Hill; Ian Anderson	Ray Hill	Ian Anderson
✓	Public-ShoeDeal	Deleted	Microsoft Team	https://avepointatsd...	Private Team Policy	Ray Hill	Ray Hill	Ian Anderson
✓	Public-SalesWestVAT	Deleted	Microsoft Team	https://avepointatsd...	Private Team Policy	Ray Hill	Barriemore Barlow	Ray Hill
✓	PublicProductXYZ	Deleted	Microsoft Team	https://avepointatsd...	Public Short Term Te...	Ray Hill	Ray Hill	Ian Anderson
⚠️	Public-PDT	Deleted	Microsoft 365 Group	https://avepointatsd...	Private Team Policy	Ian Anderson	Ian Anderson	Ray Hill
✓	Public-New Marketing	Deleted	Microsoft Team	https://avepointatsd...	Public Short Term Te...	Ian Anderson	-	Ray Hill
✓	PublicMarketingEvents	Deleted	Microsoft Team	https://avepointatsd...	Public Short Term Te...	Ray Hill	Ray Hill	Ian Anderson
🕒	Public-internal_project	Deleted	Microsoft 365 Group	https://avepointatsd...	Private Team Policy	Ray Hill	Barriemore Barlow	Ian Anderson
🕒	Public-internal_Project	Deleted	Microsoft Team	https://avepointatsd...	Private Team Policy	Ray Hill	Ray Hill	Ian Anderson
✓	Public-Internal HR Proj	Deleted	Microsoft Team	https://avepointatsd...	Public Team Policy	Ray Hill	Ray Hill	Ian Anderson
✓	PublicHRUpdates	Deleted	Microsoft Team	https://avepointatsd...	Public Team Policy	Ray Hill	Ray Hill	Ian Anderson
✓	PublicHRCommunicati	Deleted	Microsoft Team	https://avepointatsd...	Public Team Policy	Ray Hill	Ray Hill	Ian Anderson
✓	PublicGroupe-Example	Deleted	Microsoft 365 Group	https://avepointatsd...	Public Team Policy	Barriemore Barlow	\$requester	\$managerofrequester

Choose columns (14)

- Claim status
- Renewal profile
- Lifecycle information
 - Created time
 - Lease expiration time
 - Inactivity threshold time
 - Active lifecycle tasks
 - Phase assignee
 - Renewal start time
 - Renewal due date
 - Next renewal date
 - Last renewal time
- Additional Information
 - Access Level
 - Classification
 - Critical Business Application
 - Customer ID
 - Customer Name
 - Line of Service
 - Matter Approver
 - Matter Number
 - Migration Service
 - Object Type
 - Office Abbreviation
 - Office Name
 - Practice Area

Cancel Save

Admins can drill-down for all details of each workspace

The screenshot displays the Microsoft Cloud Governance interface. The top navigation bar includes the 'Cloud Governance' logo and user profile. The left sidebar contains navigation options: Home, Management (Services, Profiles, Service templates), Settings (MyHub settings, System settings), Directory (Workspace report, Guest user report), and Job monitor. The main area shows a 'Workspace report' table with columns for Phase, Name, Status, Type, Privacy, Policy, and Priority. The 'Q2 Outing' workspace is selected and highlighted. A right-hand pane titled 'View details: Q2 Outing' provides a detailed view of the selected workspace, including tabs for 'Workspace details', 'Timeline', and 'Policy info'. The 'User information' section lists Group/Team owners (Barriemore Barlow, Ray Hill), Primary Data Owner (Ray Hill), and Secondary contact (Ian Anderson). The 'Advanced information' section shows Hub details, Geo location (N/A), Storage limit (25600 GB), Storage used (0.046 GB), External sharing for site (New and existing external users), External sharing for group/team (On), Classification, Claim status (Claimed), and Renewal profile (Team Renewal). The 'Lifecycle information' section is also visible at the bottom.

Phase	Name	Status	Type	Privacy	Policy	Priority
✓	R&D Team Site	Deleted	Site Collection		SC Intranet Policy	Barriemore Barlow
✓	Quarterly Conference	Archived	Microsoft Team	Public	Internal Group Team...	Barriemore Barlow
✓	Q2 Outing	Active	Microsoft Team	Private	Guest Group Team P...	Barriemore Barlow
🕒	publictoprivate	Active	Microsoft Team	Private	-	Barriemore Barlow
✓	Public-Team_ElPaso	Deleted	Microsoft Team	Public	Private Team Policy	Ray Hill
✓	Public-ShoeDeal	Deleted	Microsoft Team	Public	Private Team Policy	Ray Hill
✓	Public-SalesWestVAT	Deleted	Microsoft Team	Public	Private Team Policy	Ray Hill
✓	PublicProductXYZ	Deleted	Microsoft Team	Private	Public Short Term Te...	Ray Hill
⚠️	Public-PDT	Deleted	Microsoft 365 Group	Public	Private Team Policy	Ian Anderson
✓	Public-New Marketing	Deleted	Microsoft Team	Public	Public Short Term Te...	Ian Anderson
✓	PublicMarketingEvents	Deleted	Microsoft Team	Private	Public Short Term Te...	Ray Hill
🕒	Public-internal_project	Deleted	Microsoft 365 Group	Public	Private Team Policy	Ray Hill
🕒	Public-internal_Project	Deleted	Microsoft Team	Public	Private Team Policy	Ray Hill
✓	Public-Internal HR Proj	Deleted	Microsoft Team	Private	Public Team Policy	Ray Hill
✓	PublicHRUpdates	Deleted	Microsoft Team	Public	Public Team Policy	Ray Hill
✓	PublicHRCommunicati	Deleted	Microsoft Team	Private	Public Team Policy	Ray Hill
✓	PublicGroupe-Example	Deleted	Microsoft 365 Group	Private	Public Team Policy	Barriemore Barlow

View details: Q2 Outing

Workspace details | Timeline | Policy info

User information

Group/Team owners: Barriemore Barlow, Ray Hill

Primary Data Owner: Ray Hill

Secondary contact: Ian Anderson

Advanced information

Hub

Geo location: N/A

Storage limit (GB): 25600

Storage used (GB): 0.046

External sharing for site: New and existing external users

External sharing for group/team: On

Classification

Claim status: Claimed

Renewal profile: Team Renewal

Lifecycle information

Admins can drill-down for all details of each workspace

The screenshot displays the AvePoint Cloud Governance interface. On the left is a navigation sidebar with categories like Home, Management, Settings, Directory, and Job monitor. The main area shows a 'Workspace report' table with columns for Phase, Name, Status, Type, Privacy, Policy, and Priority. The 'Q2 Outing' workspace is selected and highlighted. On the right, a 'View details: Q2 Outing' panel is open, showing tabs for 'Workspace details', 'Timeline', and 'Policy info'. The 'Timeline' tab is active, displaying a vertical list of events from 2021 to 2024, including renewal tasks, due dates, and manual triggers.

Phase	Name	Status	Type	Privacy	Policy	Priority
✓	R&D Team Site	Deleted	Site Collection		SC Intranet Policy	Bar...
✓	Quarterly Conference	Archived	Microsoft Team	Public	Internal Group Team...	Bar...
✓	Q2 Outing	Active	Microsoft Team	Private	Guest Group Team P...	Bar...
🕒	publictoprivate	Active	Microsoft Team	Private	-	Bar...
✓	Public-Team_ElPaso	Deleted	Microsoft Team	Public	Private Team Policy	Ray...
✓	Public-ShoeDeal	Deleted	Microsoft Team	Public	Private Team Policy	Ray...
✓	Public-SalesWestVAT	Deleted	Microsoft Team	Public	Private Team Policy	Ray...
✓	PublicProductXYZ	Deleted	Microsoft Team	Private	Public Short Term Te...	Ray...
⚠️	Public-PDT	Deleted	Microsoft 365 Group	Public	Private Team Policy	Ian...
✓	Public-New Marketing	Deleted	Microsoft Team	Public	Public Short Term Te...	Ian...
✓	PublicMarketingEvents	Deleted	Microsoft Team	Private	Public Short Term Te...	Ray...
🕒	Public-internal_project	Deleted	Microsoft 365 Group	Public	Private Team Policy	Ray...
🕒	Public-internal_Project	Deleted	Microsoft Team	Public	Private Team Policy	Ray...
✓	Public-Internal HR Proj	Deleted	Microsoft Team	Private	Public Team Policy	Ray...
✓	PublicHRUpdates	Deleted	Microsoft Team	Public	Public Team Policy	Ray...
✓	PublicHRCommunicati	Deleted	Microsoft Team	Private	Public Team Policy	Ray...
✓	PublicGroupe-Example	Deleted	Microsoft 365 Group	Private	Public Team Policy	Bar...

View details: Q2 Outing

Workspace details | **Timeline** | Policy info

Action type All | Action within 1 year

- 2024-04-01**
Next renewal: 2024-04-01 11:48:44
- 2021-08-31**
Renewal task will be assigned to: **Ian Anderson**
- 2021-08-31**
Due date
- 2021-07-13**
Renewal task will be assigned to: **Primary team contact**
- 2021-05-25**
Renewal task will be assigned to: **Secondary team contact**
- 2021-04-06 (Today)**
Renewal task is pending to be completed by **Ray Hill**
- 2021-04-06 11:50:54**
Renewal task was assigned to: **Ray Hill**
- 2021-04-06 11:48:45**
Renewal process started.
- 2021-04-06 11:48:43**
Renewal process was manually triggered by **Ian Anderson**.
- 2021-04-06 11:47:19**
Renewal process started.
- 2021-04-06 11:47:17**
Renewal process was manually triggered by **Ian Anderson**.
- 2021-04-06 11:44:54**
Renewal process started.
- 2021-04-06 11:44:53**

Admins can drill-down for all details of each workspace

The screenshot displays the AVEVA Cloud Governance interface. The top navigation bar includes the AVEVA logo, 'Cloud Governance', and utility icons for settings, help, and user profile. The left sidebar contains navigation options: Home, Management (Services, Profiles, Service templates), Settings (MyHub settings, System settings), Directory, Workspace report (selected), Guest user report, and Job monitor.

The main content area shows a 'Workspace report' table with columns for Phase, Name, Status, Type, Privacy, Policy, and Priority. The 'Q2 Outing' workspace is highlighted. Below the table, a 'View details: Q2 Outing' panel is open, showing three tabs: 'Workspace details', 'Timeline', and 'Policy info' (selected). The 'Policy info' tab displays various settings for the workspace, including sharing options and access requests.

Phase	Name	Status	Type	Privacy	Policy	Priority
✓	R&D Team Site	Deleted	Site Collection		SC Intranet Policy	Bar...
✓	Quarterly Conference	Archived	Microsoft Team	Public	Internal Group Team...	Bar...
✓	Q2 Outing	Active	Microsoft Team	Private	Guest Group Team P...	Bar...
🕒	publictoprivate	Active	Microsoft Team	Private	-	Bar...
✓	Public-Team_ElPaso	Deleted	Microsoft Team	Public	Private Team Policy	Ray...
✓	Public-ShoeDeal	Deleted	Microsoft Team	Public	Private Team Policy	Ray...
✓	Public-SalesWestVAT	Deleted	Microsoft Team	Public	Private Team Policy	Ray...
✓	PublicProductXYZ	Deleted	Microsoft Team	Private	Public Short Term Te...	Ray...
⚠️	Public-PDT	Deleted	Microsoft 365 Group	Public	Private Team Policy	Ian...
✓	Public-New Marketing	Deleted	Microsoft Team	Public	Public Short Term Te...	Ian...
✓	PublicMarketingEvents	Deleted	Microsoft Team	Private	Public Short Term Te...	Ray...
🕒	Public-internal_project	Deleted	Microsoft 365 Group	Public	Private Team Policy	Ray...
🕒	Public-internal_Project	Deleted	Microsoft Team	Public	Private Team Policy	Ray...
✓	Public-Internal HR Proj	Deleted	Microsoft Team	Private	Public Team Policy	Ray...
✓	PublicHRUpdates	Deleted	Microsoft Team	Public	Public Team Policy	Ray...
✓	PublicHRCommunicati	Deleted	Microsoft Team	Private	Public Team Policy	Ray...
✓	PublicGroupe-Example	Deleted	Microsoft 365 Group	Private	Public Team Policy	Bar...

View details: Q2 Outing

Workspace details | **Timeline** | **Policy info**

Policy info

- Allow users to share the group team site content with people outside the organization: New and existing external users
- Allow members to share the site and individual files and folders: Yes
- Allow members to invite others to the site members group: Yes
- Allow access requests: Yes
- Send access requests to: The site owners group
- Custom message shown on the access request page

Group/Team lifecycle management >

Group/Team inactivity threshold management v

- Enable group/team inactivity threshold: 3 years
- Approval process: IA Approval
- Enable group/team inactivity threshold warning: Yes
- Reminder profile: Team Expiration Warning
- Enable an additional group/team lifecycle action: No

Group/Team lease management >

EXAMPLE

“Policies” are defined and mapped to users, divisions, or purpose

	ITAR/EAR Protected Workspace	General Purpose Workspace	CAS Protected Workspace
Team Owner	Service Account	Business User	Service Account
EXPIRATION/ RETENTION	3 Months after last accessed	3 Months after last accessed	12 Months after last accessed
MEMBER SHARING SETTINGS	Not Allowed	Allowed	Not Allowed
RECERTIFY ACCESS	after 3 Months	after 6 Months	after 12 Months

How do you get there from here?

Managed provisioning or import of collaborative workspaces



How do you keep this information current over time?

Periodic review and confirmation of permissions, access, ownership and key governance attributes



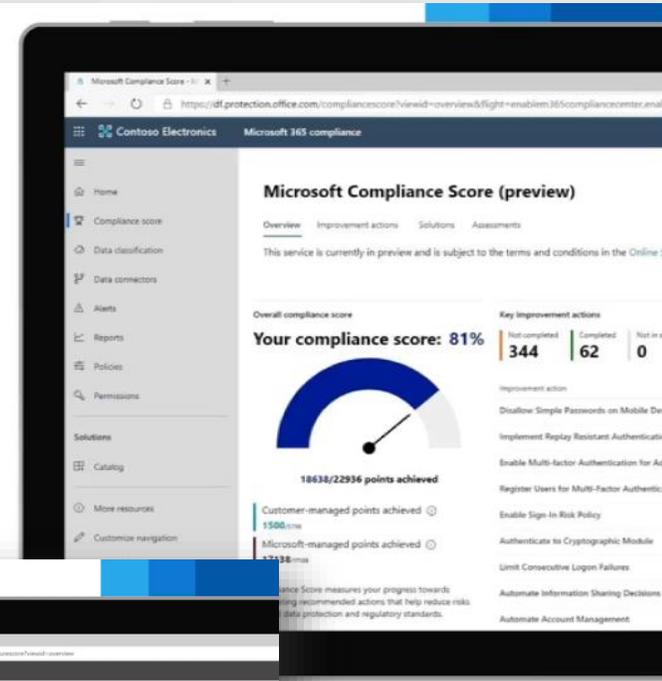
What can you do today?

Microsoft has some great out of the box score cards to understand your current posture.



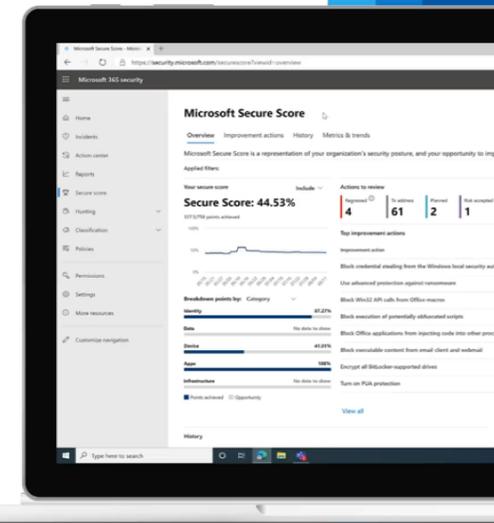
Microsoft 365 Security

Compliance Score



Microsoft Secure Score

Strengthen your security posture





Licensing: Greatest Hits from Microsoft



Breakdown of basic & advanced use cases by SKU

Quick reference:

Manual = E3

Automated = E5

Microsoft 365 licensing guidance for security & compliance

Microsoft 365 licensing guidance for security & compliance

Plan for Microsoft 365 compliance - DoD deployments

Plan for Microsoft 365 compliance - GCC High

Plan for Microsoft 365 compliance - GCC



Next Steps!

Resources to dig in deeper on today's topics...



Feel Free to Reach out!



Michael.Wit@avepoint.com



www.linkedin.com/in/mike-wit

See Policies and Insights in action! How to videos available here...

<https://youtu.be/kgbnQvl-sFc>

Whitepaper: Implementing a Best Practice Approach to Risk-Based Data Protection and Cybersecurity

<https://www.avepoint.com/resources/whitepaper-form/4429>

Request a demonstration of the AvePoint solutions discussed today!

<https://www.avepoint.com/get-started>



AvePoint

Policies & Insights

For Microsoft 365



AvePoint

White papers

Operational Governance Transform IT delivery into business success.

Increase IT efficiency and transparency. Accelerate user adoption. Drive value with Office 365 and SharePoint.

Get Started Today

*thank
you*



Sales@AvePoint.com | +1 800.661.6588



www.AvePoint.com



[in](#) [🐦](#) [▶](#) [f](#)