



Office 365 Security Concerns: Stop Data Leaks / Insider Attacks

Protecting sensitive data doesn't need to slow down your organization's ability to share and collaborate



Unleash the Power of You

Accessible content is available upon request.



Migrate. Manage. Protect.



12 Global Cloud Instances

99.5% Availability Backed by Azure

24/7 World-Class Support

50PB+ Managed Customer Data

ISO Certification



27001:2013

16K
Customers

7M
Cloud Users

88
Countries

7
Continents

AvePoint® is headquartered and maintains its principal operational center in Jersey City, NJ, with approximately 1,500 employees across five continents.

Microsoft
Partner



2017 Partner of the Year Winner
Public Sector: Microsoft CityNext Award

2016 Partner of the Year Winner
Technology for Good Citizenship Award

2015 Partner of the Year Winner
Collaboration and Content

2014 Partner of the Year Winner
Public Sector: Public Safety and National Security



Today's Speakers



John Hodges

SVP of Product Strategy

John is focused on developing solutions that address modern data protection needs for organizations worldwide, working with many Fortune 500 companies to drive sustainable adoption of Microsoft technology.



Hunter Willis

Product Marketing Manager

Hunter is the President of the Richmond SharePoint User Group. He is a top contributor for AvePoint's blog as well as CMS Wire, and has been featured in over a dozen publications, most notably the Wall Street Journal.



Agenda – Protecting Sensitive Data



WHO: Who has access?

- Overview of direct sharing in Teams
- Overview of sharing with external users / guest accounts
- Overview of AD Groups vs. Microsoft 365 groups

WHAT: Defining risk and finding data!

- Define “sensitivity” for content
- Native discovery options (for E5/M5 customers)
- Native content search (for all ‘E’ license levels)

HOW: Building and tracking policies!

- Natively applying DLP / Sensitivity Policies
- Summarizing this data
- Scoping and applying policies



Why are we here? Regulatory Pressure!

Access Controls & Role Separation

Determine the cross section of your data that needs to be tightly controlled from access to foreign nationals or entities

Oversight on End User Activity

Detailed activity logs and on-demand reports available to always know how files are being accessed or shared

Data Sovereignty & Geofencing

Ensure that data repository site is hosted in the US and that all employees of both provider and data center are US citizens

Data Inventory & Mapping

Identify and classify data throughout its entire lifecycle in order to assess individual risk and governance (i.e. USML, MTCR, etc...)

Maintain Relevancy of Data

Ensure proper data purging for the purposes of removing redundant and obsolete data through automated lifecycle policies

Validation on Reasonable Efforts

Proof of having methods to identify ALL sensitive data, security policies and practices to protect it, and ability to resolve violations

Examples...

ISO 27001
ITAR
GDPR



Why are we here?

How difficult are ISO certs and security team audits?



Permissions reports &
security searches



Where and how is sensitive
content being used



How do I validate my
collaboration is secure



With research we can try to find

What does Roy (ext) have access to?

Permissions Reports

An external user (Roy) has access to this Team.

Has Roy accessed anything?

Audit Reports

A document has been accessed 10 times in the past month.

Is anything that's been accessed sensitive?

DLP Reports

This Team contains sensitive information

to



Roy, an external user, has access to confidential info and has accessed it 10 times this past month.



Who has access?

Teams, Groups, Sites, oh my...

Where is my source of truth for “who has access”?



Teams vs. SharePoint access...

The same, right?!

Permissions

Manage site permissions or invite others to collaborate

Invite people

- Site owners
- Site members

- Adele Vance
Edit
- Alex Wilber
Edit
- Allan Deyoung
Edit
- Christie Cline
Edit

Members Channels Analytics Apps

Search for members

Owners (2)

Members and guests (22)

Name	Title	Location
Enrico Cattaneo	Attorney	14/1102
Pradeep Gupta	Accountant	98/2202
Emily Braun	Budget Analyst	97/2302
Alex Wilber	Marketing Assistant	131/1104

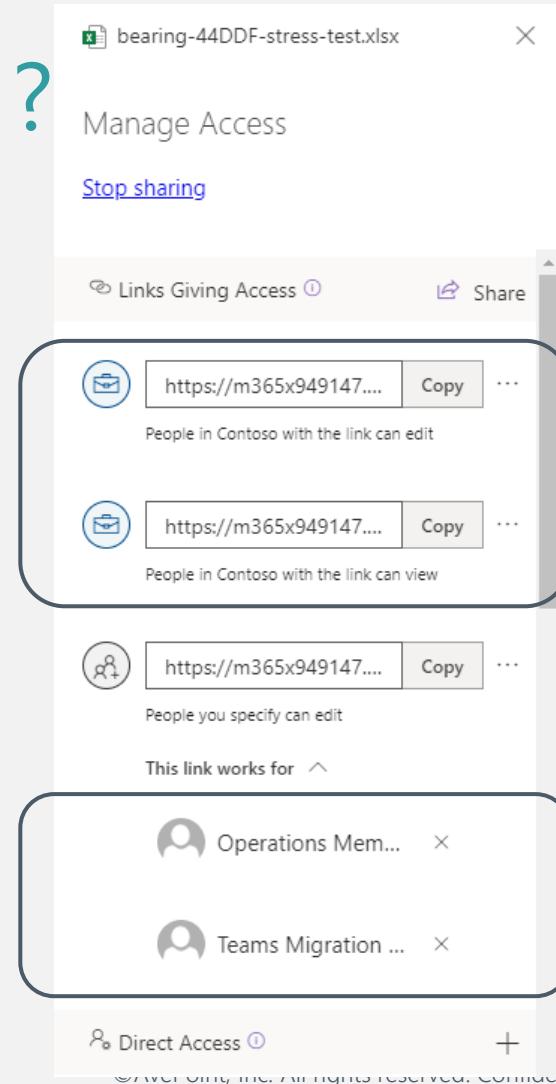


Teams, Groups, Sites, oh my...

Where is my source of truth for “who has access”?



The files say... ?



Where were these links pasted?

Who is/was in these groups?



“Who has access”... Sharing is caring!

And it's easy



Sharing buttons in Office Apps

The screenshot shows the Microsoft PowerPoint interface with the 'Link settings' dialog box open. The dialog box is titled 'Link settings' and shows options for sharing the presentation. The 'People in your organization with the link' option is selected. The 'Allow editing' checkbox is checked, and the 'Block download' toggle is off. The 'Apply' button is highlighted.



"Who has access"... Sharing is caring!

And it's easy



OneDrive: Teams 1-1 and Office Apps

The screenshot displays the OneDrive web interface. At the top, the user profile for Emily Braun is shown with tabs for Chat, Files, Organization, and Activity. The 'Files' tab is active, showing a list of files. A file named 'About AvePoint_2019.pptx' is highlighted. To the right, the 'Microsoft Teams Chat Files' section shows the same file, 'About AvePoint_2019.pptx', with a 'Modified' timestamp of '8 minutes ago' and 'Modified By' as 'MOD Administrator'. The interface includes various action buttons like 'Open', 'Get link', 'Download', 'Share', 'Copy link', 'Sync', 'Download', and 'Automate'.



"Who has access"... Sharing is caring!

And it's easy



Private Channels in Teams

The screenshot displays the Microsoft Teams interface. On the left, the 'Teams' sidebar shows 'Your teams' with 'X1050 Launch Team' selected. Under this team, several channels are listed: 'General', 'Design', 'Digital Assets Web', 'Distribution' (marked with a lock icon), and 'Vendor Security Channel' (also marked with a lock icon). A dashed line connects the 'Distribution' channel in the sidebar to the main content area. The main content area shows the 'X1050 Launch Team - Distribution' channel. At the top, there's a search bar and a 'Search or type a command' input. Below this, the channel name 'X1050 Launch Team - Distribution' is displayed. A navigation pane on the left lists 'Home', 'Documents', 'Parent Team', 'Pages', 'Site contents', 'Recycle bin', and 'Edit'. The 'Documents' section is active, showing a message: 'This folder is connected to a channel in Microsoft Teams'. Below this, the breadcrumb 'Documents > Distribution' is shown. A table lists documents within the channel:

Name	Modified	Modified By
Governance-Cloud-First.pptx	A few seconds ago	MOD Administrator



"Who has access"... Sharing is caring!

And it's about to get easier!



Stream Enhancements (Ignite 2020)

- Recordings & videos now behave like files!



Patrick Guimonet #Power365 #aOSNice @patricg · 50m

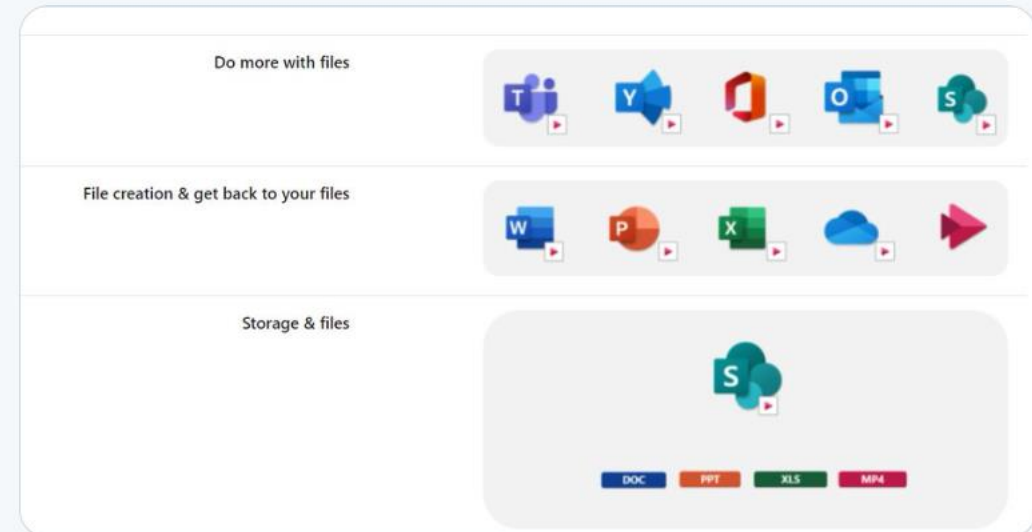
Great new capabilities coming to #Stream as #videos will be directly stored in #OneDrive and #SharePoint

At last we will be able to share videos via anonymous links !!!

More details here: lnkd.in/dtDjVKb

and in this session lnkd.in/dVJKX9s

#microsoft365



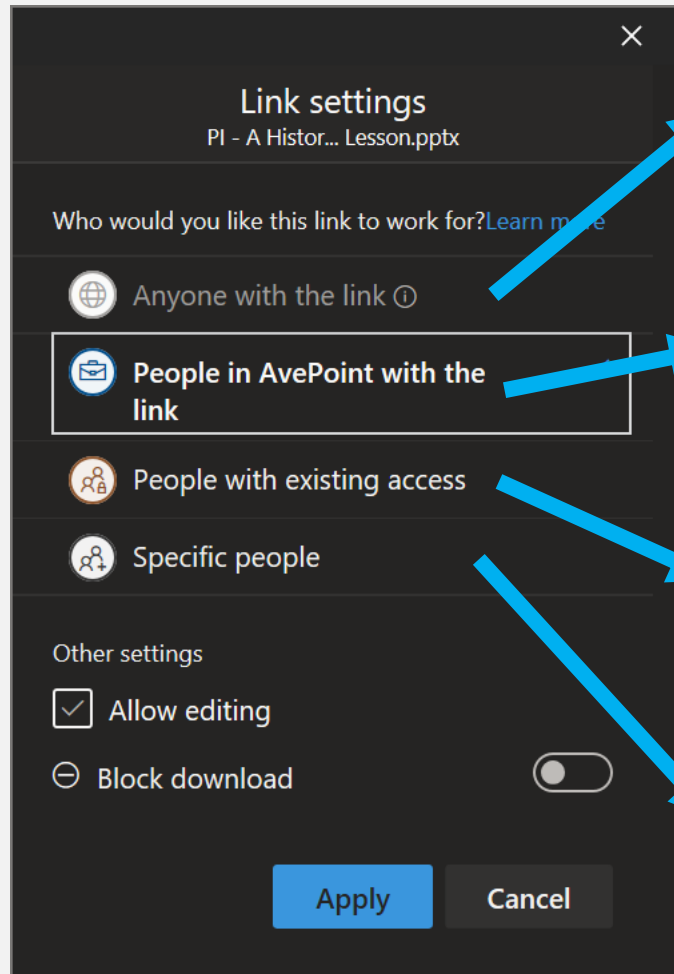
1

5

6



Reminder: How we got here



Anonymous & External Links

So Easy! "Everyone except external"

Large and Nested Security Groups

Explicit people hiding in the wings



Teams "Files" are really SharePoint files...

The screenshot displays the Microsoft Teams interface for a group named "BGLeads". On the left, a sidebar lists channels: Activity, Chat (with 2 messages), Teams, Meetings, and Calls. The main area shows the "General" channel selected. Below the channel name, a list of channels is visible: BG Virtual Stand-up, BG-Dev Workshop 2018, GTM-Sales, Product Strategy, Project Tasks, SP 2019, Technical Partnerships, and a link for "2 more channels". On the right, the "Documents" section shows a list of files. Red arrows connect the channel names in the left sidebar to the corresponding folder names in the "Documents" list, illustrating that Teams channels are backed by SharePoint documents.

Channel	Document Name	Modified
BG Virtual Stand-up	BG Virtual Stand-up	July 16
BG-Dev Workshop 2018	BG-Dev Workshop May 2018 C...	April 24
GTM-Sales	Field Feedback	March 15
Product Strategy	General	November 17, 2017
Project Tasks	GTM-Sales	August 14, 2017
SP 2019	Product Strategy	August 14, 2017
Technical Partnerships	Project Tasks	6 days ago
	SP 2019	July 3
	Technical Partnerships	August 14, 2017



It's about to get worse....

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 ☒ On

Choose who will receive access requests for this site:

- ☒ BGLeads Owners
- ☐ Specific email

Add a custom message to the request access page:

For example: Please allow three days for us to review your request.

Save

Discard

Site Information

Site logo

 Change

Site name *

BGLeads

Site description

Business Group Leads

Privacy settings

- Private - only members can access thi... ▾
- Private - only members can access this site
- Public - anyone in the organization can acce

[View all site settings](#)

 [Delete site](#)

Save

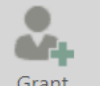
Cancel

BROWSE

PERMISSIONS

BROWSE

PERMISSIONS



Grant Permissions



Create Group



Edit User Permissions

Grant

Home

Conversations

News

Documents

Notebook

Recent

19:b2e8d2185925493b9
df22133b760c2ed@thre
ad.skype_wiki

19:540ee0e142164a50b
eb8d50b16d77496@thr
ead.skype_wiki

19:76580ceee9af4105b2
ba331a99b6d175@thre
ad.skype_wiki

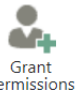
19:c66630b0b38b48aeb
ade1d0de0745ae0@thr
ead.skype_wiki

Tasks 1

BG Pursuit Requests

Pages

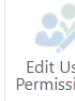
Legacy Documents



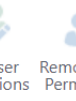
Grant



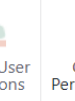
Create Group



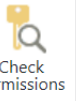
Edit User Permissions



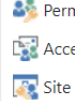
Remove User Permissions



Check



Access Request Settings



Site Collection Administrators

Permission Levels

Access Request Settings

Site Collection Administrators

Manage

Home

Conversations

News

Documents

Notebook

Recent

19:b2e8d2185925493b9
df22133b760c2ed@thre
ad.skype_wiki

19:540ee0e142164a50b
eb8d50b16d77496@thr
ead.skype_wiki

19:76580ceee9af4105b2
ba331a99b6d175@thre
ad.skype_wiki

19:c66630b0b38b48aeb
ade1d0de0745ae0@thr
ead.skype_wiki

Tasks 1

BG Pursuit Requests

Pages

Legacy Documents

BG Enablement Docs

BG Example Docs

BG Initiatives Tracking

BG Lead Activity Calendar

BG_Workstream Projects

BG_Workstreams

Shared wExec Leadership-



Name



Aaron Barnes



Ada Liu



Alex Gasper



Alfred Lombardi



Alyssa Blackburn



Andrew Diaz



AnnMarie Connolly



AOS Product PM Members



Architects



Armand Zhou



Austin Han



Baron Zhang



BG Enablement Contributors



BG Members



BG Owners



BG Visitors



BG+PMK



BGLeads Members



BGLeads Owners



BGLeads Visitors



Blake Zhang

Type

User

User

User

User

User

User

User

Domain Group

Domain Group

User

User

User

SharePoint Group

SharePoint Group

SharePoint Group

SharePoint Group

Domain Group

SharePoint Group

SharePoint Group

SharePoint Group

User

Permission Levels

Limited Access

Limited Access

Limited Access

Limited Access

Limited Access

Limited Access

Limited Access

Limited Access

Limited Access

Limited Access

Limited Access

Limited Access

Limited Access

Limited Access

Limited Access

Limited Access

Limited Access

Edit, Limited Access

Full Control, Limited Access

Read, Limited Access

Limited Access

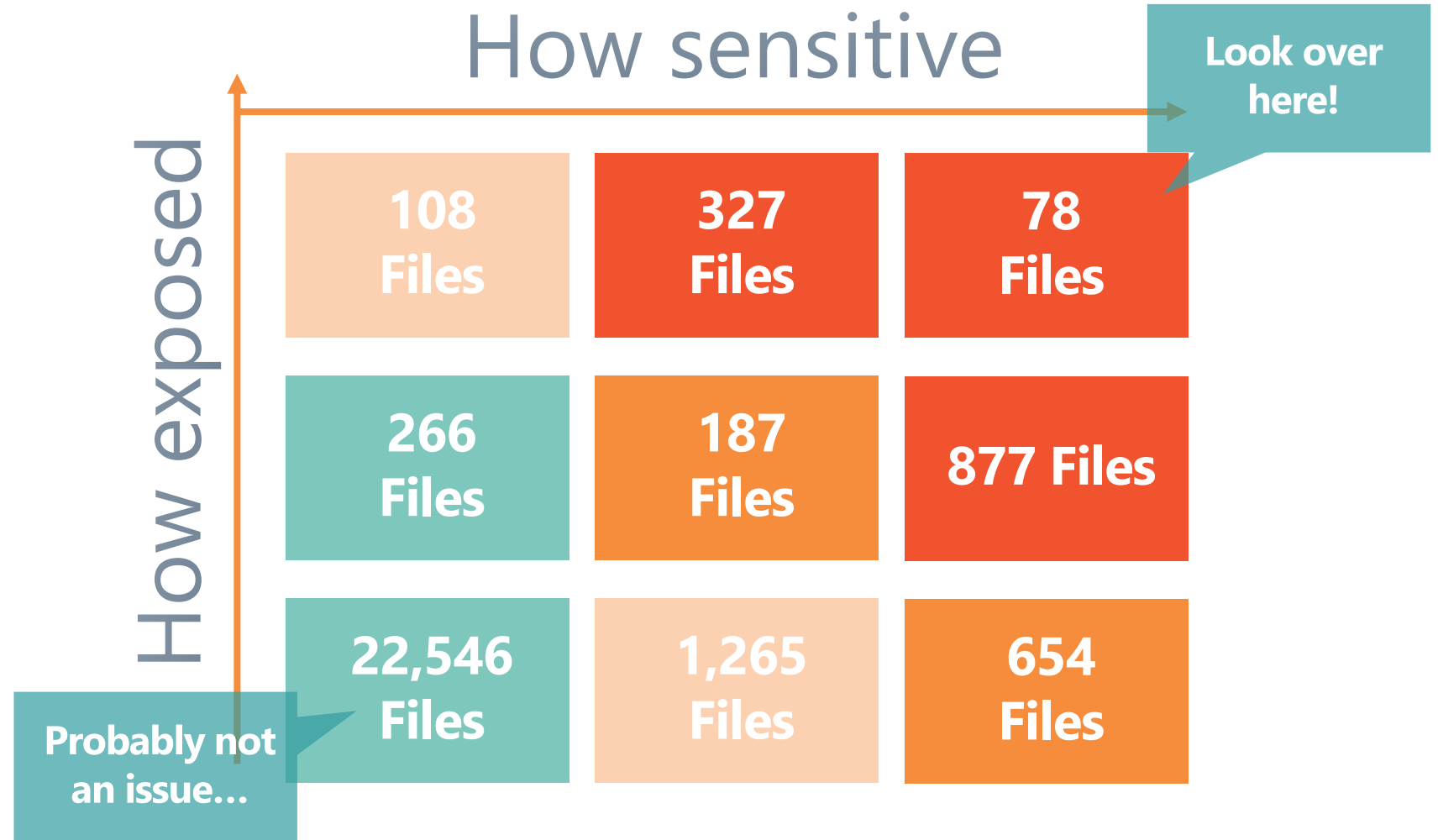
WHO?



How do we define risk?

What do I gain?

Focus only on what's important, ignore the noise.



Context helps save time and effort responding to security team requests. Focus only on what matters most.



Identifying Sensitive Data Natively

Microsoft 365 compliance

Home

Compliance score

Data classification

Data connectors

Alerts

Reports

Policies

Permissions

Data classification

[Overview](#)[Trainable classifiers \(preview\)](#)[Sensitive info types](#)[Content explorer](#)[Activity explorer](#)

Get snapshots of how sensitive info and labels are being used across your organization's locations, including any files that [more](#)

Top sensitive info types

Sensitive info types used most in your content

International Classification of Diseases (ICD-10-CM)	International Classification of Diseases (ICD-9-CM)	Credit Card Number	EU Debit Card Number	U.S. Social Security Number (SSN)	U.S. Bank Account Number
--	---	--------------------	----------------------	-----------------------------------	--------------------------



Sensitive Information Types are the Key!

Microsoft 365 compliance

Data loss prevention > Create policy

Choose the information to protect

Name your policy

Locations to apply the policy

Policy settings

Test or turn on the policy

Review your settings

Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later. [Learn more about DLP policy templates](#)

Search

Show options for All countries or regions

42 results

Financial

Medical and health

Privacy

Custom

PCI Data Security Standard (PCI DSS)

Saudi Arabia - Anti-Cyber Crime Law

Saudi Arabia Financial Data

U.K. Financial Data

U.S. Financial Data

U.S. Federal Trade Commission (FTC) Consumer Rules

U.S. Gramm-Leach-Bliley Act (GLBA)

U.S. Financial Data

Description

Helps detect the presence of information commonly considered to be financial information in United States, including information like credit card, account information, and debit card numbers.

Protects this information:

- Credit Card Number
- U.S. Bank Account Number
- ABA Routing Number

Sensitive Info
Types are PRE-
INDEXED for
use in policies!



Creating a Content Search for Sensitive Info

The screenshot illustrates the process of creating a content search in the Office 365 Security & Compliance center. The interface is divided into several sections:

- Navigation Panel (Left):** Contains links to Home, Alerts, Permissions, Classification, Data loss prevention, Records management, Information governance, Supervision, Threat management, Mail flow, Data privacy, and Search. The **Content search** link is highlighted with an orange box and an arrow.
- Main Content Area:**
 - Searches Tab:** Displays a "Search query" section with a "Keywords" input field (containing "SensitiveType: 'Credit Card Number'") and a "Show keyword list" checkbox. Below this is an "Add conditions" button.
 - Exports Tab:** Shows a "New search" section with a "Name your search" checkbox (checked), a "Choose locations" checkbox (checked), and a "Create query" radio button (selected).
- Condition Card (Right):** A modal window titled "Condition card" with a "Keywords" section containing the same search query and a "Show keyword list" checkbox. Below this is an "Add conditions" button and "Back", "Finish", and "Cancel" buttons.

At the bottom of the interface, there are sections for "SharePoint sites" (None selected) and "OneDrive accounts" (Choose sites), each with "Back", "Next", and "Cancel" buttons.

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

How do we build policies?

Better Stories = Stronger Policies

From

An external user (Roy) has access to this Team.

A document has been accessed 10 times in the past month.

This Team contains sensitive information

to



Roy, an external user, has access to confidential info and has accessed it 10 times this past month.

Now let's restrict his access with a policy that blocks external users Roy from "sensitive" Teams!

to



Sarah granted Roy access to this file, but we reverted it and sent Sarah a notification as to why.



With research we can try to find

What does Roy (ext) have access to?

Permissions Reports

An external user (Roy) has access to this Team.

Has Roy accessed anything?

Audit Reports

A document has been accessed 10 times in the past month.

Is anything that's been accessed sensitive?

DLP Reports

This Team contains sensitive information

to



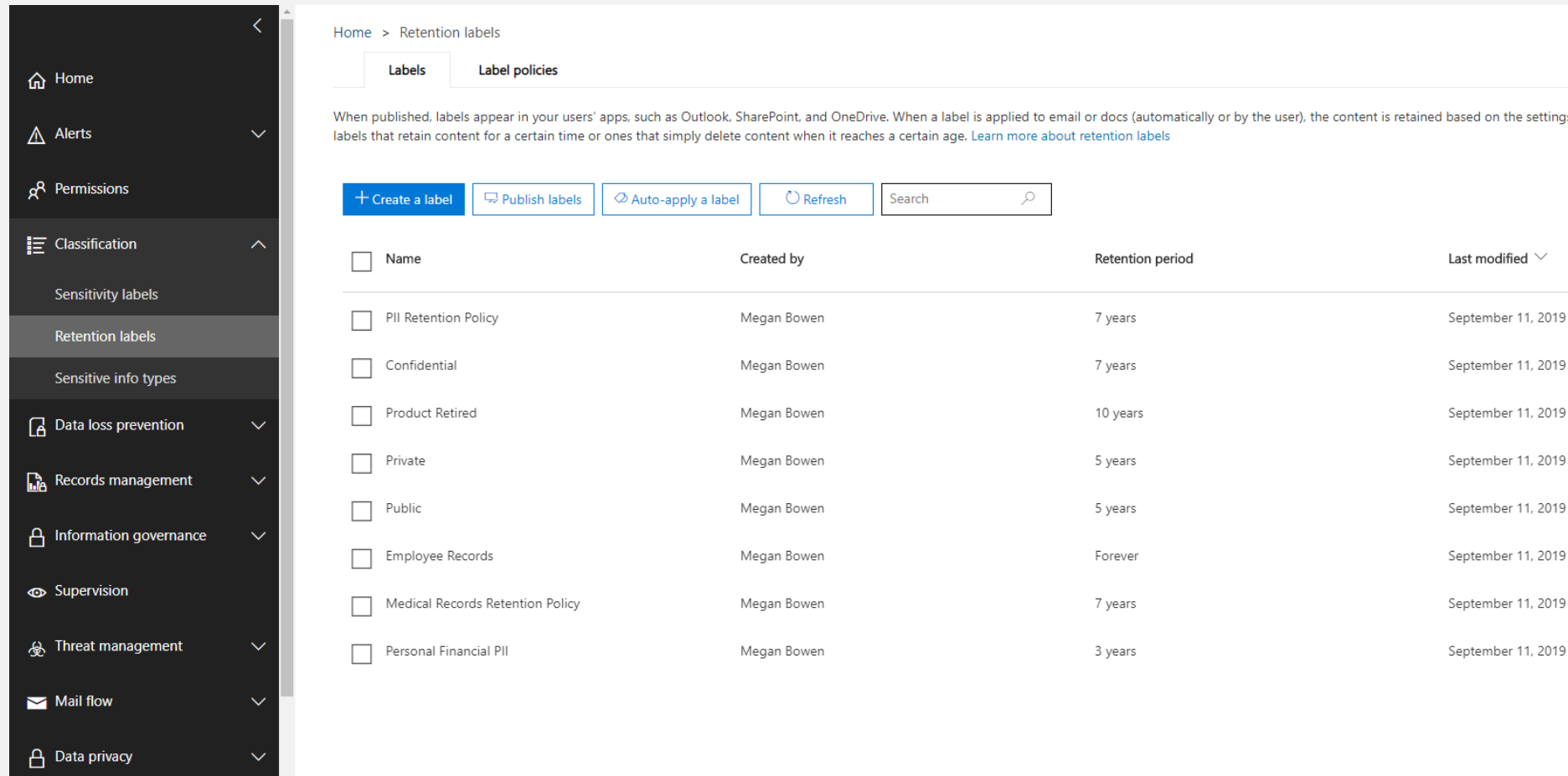
Roy, an external user, has access to confidential info and has accessed it 10 times this past month.



Retention and Sensitivity Labels

Lock files
based on
sensitivity.

Can apply to
specific
locations in
O365



Home > Retention labels

Labels Label policies

When published, labels appear in your users' apps, such as Outlook, SharePoint, and OneDrive. When a label is applied to email or docs (automatically or by the user), the content is retained based on the settings labels that retain content for a certain time or ones that simply delete content when it reaches a certain age. [Learn more about retention labels](#)

[+ Create a label](#) [Publish labels](#) [Auto-apply a label](#) [Refresh](#)

<input type="checkbox"/> Name	Created by	Retention period	Last modified
<input type="checkbox"/> PII Retention Policy	Megan Bowen	7 years	September 11, 2019
<input type="checkbox"/> Confidential	Megan Bowen	7 years	September 11, 2019
<input type="checkbox"/> Product Retired	Megan Bowen	10 years	September 11, 2019
<input type="checkbox"/> Private	Megan Bowen	5 years	September 11, 2019
<input type="checkbox"/> Public	Megan Bowen	5 years	September 11, 2019
<input type="checkbox"/> Employee Records	Megan Bowen	Forever	September 11, 2019
<input type="checkbox"/> Medical Records Retention Policy	Megan Bowen	7 years	September 11, 2019
<input type="checkbox"/> Personal Financial PII	Megan Bowen	3 years	September 11, 2019



SharePoint, OneDrive, and other “Sites”

External sharing

Content can be shared with:

SharePoint	OneDrive
Most permissive	Anyone Users can share files and folders using links that don't require sign-in.
	New and existing guests Guests must sign in or provide a verification code.
	Existing guests Only guests already in your organization's directory.
Least permissive	Only people in your organization No external sharing allowed.

You can further restrict sharing for each individual site and OneDrive. [Learn how](#)

More external sharing settings ▾

File and folder links

Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive.

☐ Specific people (only the people the user specifies)

☐ Only people in your organization

☒ Anyone with the link

Choose the permission that's selected by default for sharing links.

☐ View

☒ Edit

Choose expiration and permissions options for Anyone links.

☐ These links must expire within this many days

Restrict external sharing and control provisioning. This can hamper adoption...



HR Teams



Legal Teams



Distribution

...but they will do what they need to do to get the job done. This is why Shadow IT happens.



The Teams admin center has some controls...

The screenshot displays the Microsoft Teams admin center interface. On the left is a dark sidebar with navigation options: Dashboard, Teams, Manage teams, Teams policies, Devices, Locations, Users, Meetings, Messaging policies, Teams apps, Voice, Policy packages, Analytics & reports, Org-wide settings, Planning, Legacy portal, and Call quality dashboard. The main content area has three tabs: Members (selected), Channels, and Settings. The Members tab shows a list of 24 team members with columns for Display name, Username, and Title. Below the list, there are settings for 'Discover private teams' and 'Create private channels', both set to 'On'. A dropdown menu for 'Microsoft apps' is open, showing four options: 'Allow all apps' (selected), 'Allow all apps' (with a description), 'Allow specific apps and block all others' (with a description), and 'Block specific apps and allow all others' (with a description). At the bottom, there is a toggle for 'Allow guest access in Teams' set to 'On'.

✓	Display name ↑	Username	Title
	MOD Administra...	admin@M365x949147.On...	The Big Boss
	Pradeep Gupta	PradeepG@M365x949147....	Accountant
	Patti Fernandez	PattiF@M365x949147.On...	President
	Joni Sherman	JoniS@M365x949147.On...	Paralegal
	Christie Cline	ChristieC@M365x949147....	Buyer
	Alex Wilber	AlexW@M365x949147.On...	Marketing Assistant
	Debra Berger	DebraB@M365x949147.O...	Administrative Assis
	Johanna Lorenz	JohannaL@M365x949147....	Senior Engineer
	Enrico Cattaneo	EnricoC@M365x949147.O...	Attorney
	Allan Deyoung	AllanD@M365x949147.On...	IT Admin
	Nestor Wilke	NestorW@M365x949147....	Director
	Adele Vance	AdeleV@M365x949147.O...	Retail Manager
	Isaiah Langer	IsaiahL@M365x949147.On...	Sales Rep
	Irvin Sayers	IrvinS@M365x949147.On...	Project Manager
	Emily Braun	EmilyB@M365x949147.On...	Budget Analyst

Discover private teams

☒ On

Create private channels

☒ On

Microsoft apps

Choose which Teams apps published by Microsoft or its partners can

- ☒ Allow all apps
- ☒ Allow all apps
Users can install and use any app published by Microsoft in the Teams App store.
- ☒ Allow specific apps and block all others
Allow specific apps you want to allow from the store and all other ones would be blocked.
- ☐ Block specific apps and allow all others
Add which apps you want to block from the store and all the other ones would be allowed.
- ☐ Block all apps
Users can't install any apps published by Microsoft in the Teams Apps store.

Allow guest access in Teams ☒ On

...and a few on who can potentially be added to which Teams, or what kind of content can be where.



The importance of a layered approach!

If you need “real-time” protection...

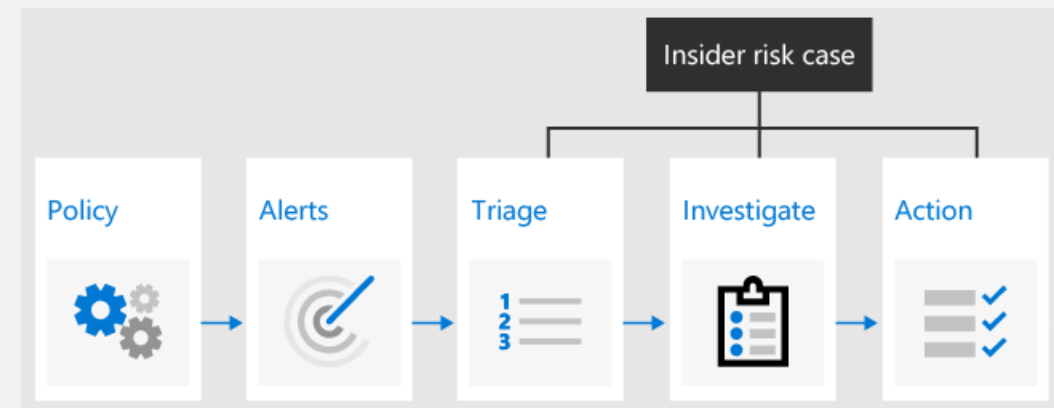
Data Loss Protection (DLP) /
Cloud App Security (MCAS)



<https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide>

If you need “suspicious behavior” detection...

Insider Risk Management (IRM)



<https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide>





 AvePoint[®]

Policies & Insights

For Microsoft 365



How can we solve the problem with AvePoint?



- Aggregate access, sensitivity, and activity data
- Regulations and information types define risk
- Prioritize to easily expose issues – focus on what matters



- Security dashboards highlight anonymous links and exposed sensitive data
- Drill down on known and potential issues
- Fix as you go – edit permissions in batch



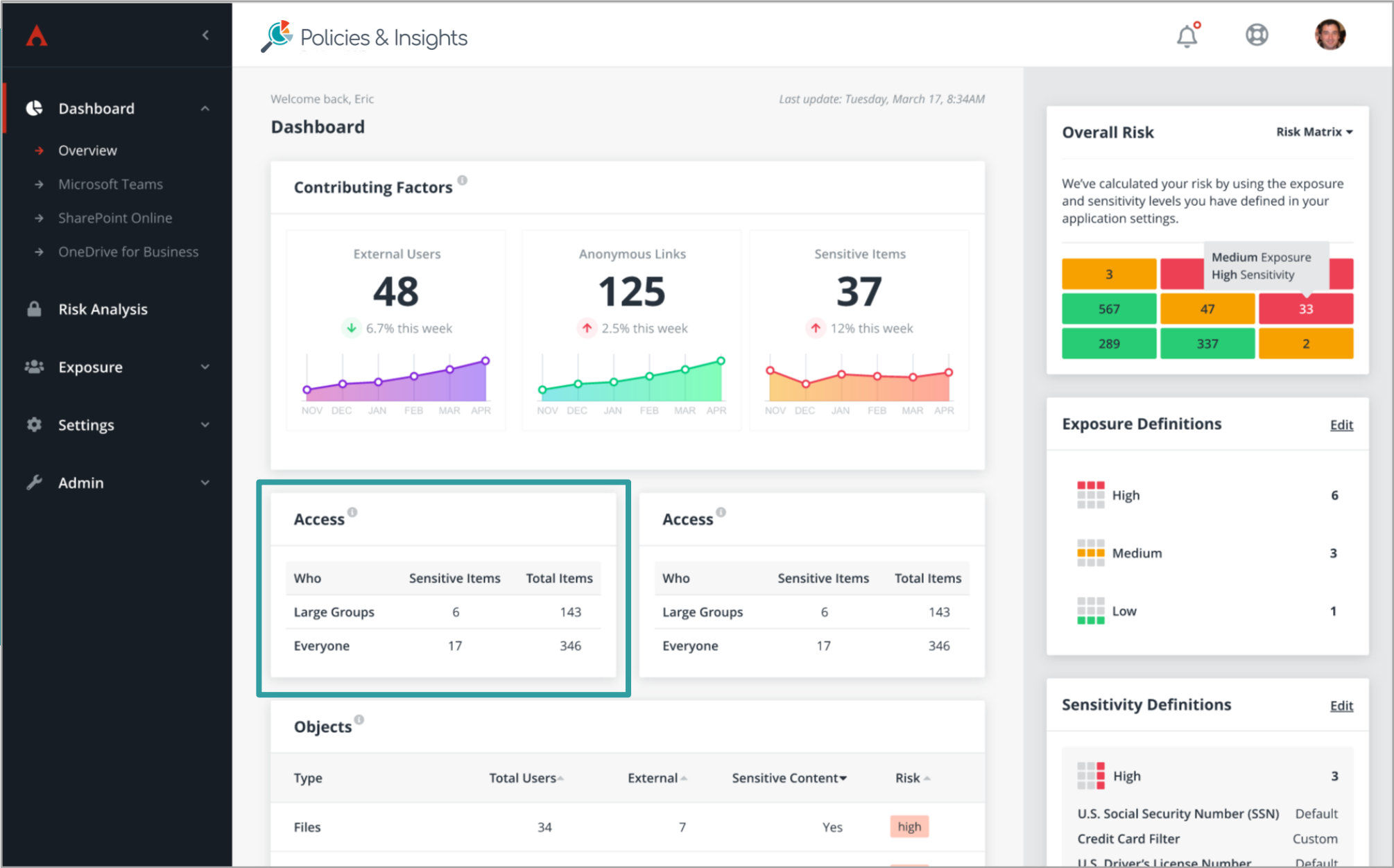
- Prevent configuration drift with automated policies
- Trigger alerts or roll-back of unauthorized changes
- Track improvements over time – prove your collaboration is secure!



Highlighting
high-risk
scenarios in
your
environment

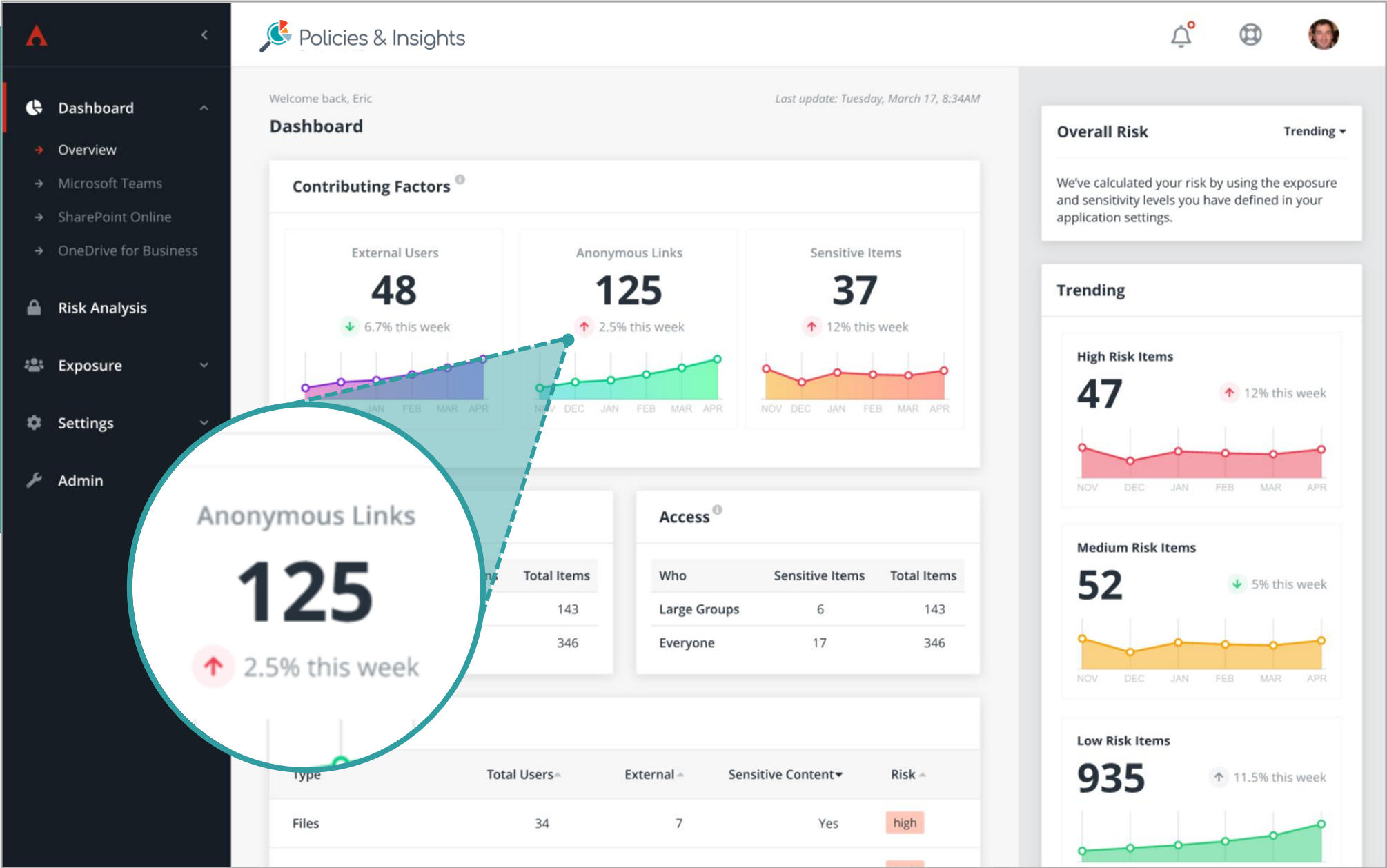
Reducing false-
positives by
working with
native Microsoft
sensitive
information
types*

*(Office 365 E3 feature)



Tracking risk over time to understand changes to your environment

Proactive policy enforcement for Groups, Teams, and other services to protect content



Cached Permissions support quick-reports on Users, Groups, Teams, Anonymous Links, and External Users

Integration with Cloud Governance Renewals for Permission Reporting

Dashboard

Risk Analysis

Exposure

→ Everyone

→ External Users

→ Large Groups

→ Anonymous Links

Settings

Admin

Policies & Insights

Exposure \ External Users

← John Hodges

Access Report

Known Risk (Direct) Possible Risk (Indirect)

Explore

Search...

<input type="checkbox"/>	Name	Object Type	Owner	Discovered on
<input type="checkbox"/>	Testing	Site Collection	Jessica Norman	03/25/2020 10:41am
<input checked="" type="checkbox"/>	Collab2020	Site Collection	Jessica Norman	03/25/2020 10:41am
<input type="checkbox"/>	Fin_Serv	Site Collection	Kelly Oleary	03/25/2020 10:41am
<input type="checkbox"/>	Human Resources	Site Collection	Tim Trotter	03/25/2020 10:41am
<input type="checkbox"/>	NA_Services	Site Collection	Liz Young	03/25/2020 10:41am

John Hodges

Access by Risk Level

Known Risk

This includes items in which this user has been given explicit access to. That includes files shared directly with this user, groups and teams this user was made a member of, etc.

High 1Medium 2Low 9

Total Items 12

Possible Risk

This is a list of all the groups this user has access to. There may be implicit risk associated with the files in each group.

Groups 12

User Activity

Accessed file

jessica_compliancedetector_com_STThumb.jpg

Just now

Viewed page

/sites/LeoJiangGroup

6 hours ago

Added site collection admin

Jessica@compliancedetector.com

A week ago

Applying corrective actions.

From

An external user (Roy) has access to this Team.

A document has been accessed 10 times in the past month.

This Team contains sensitive information

to



Roy, an external user, has access to confidential info and has accessed it 10 times this past month.

Now let's restrict his access with a policy that blocks external users Roy from "sensitive" Teams!

to



Sarah granted Roy access to this file, but we reverted it and sent Sarah a notification as to why.



Craft policies that can adapt to the way your teams work and block the most common risks in your Microsoft 365 environment!

<

Policies & Insights

Policy Management

Create Policy

Create Policy

General Information

A policy allows you to monitor violations and changes using policy rules.

* Object Type

Microsoft Teams

* Name

Copy from an existing policy

Create a new policy

No more external sharing!

Description

Rules

Other Settings

* Scan Interval

1

Days

* Retention Duration

How many days would you like to retain the data associated with this policy?

Add Rule to Microsoft Teams

Select a rule to add to the policy:

External Sharing Settings

Classification Protection

External Sharing Settings

Membership Restriction

Office 365 Group Visibility in Outlook Client

Ownership Restriction

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

☐ Include Microsoft Teams owners

Cancel

Add to Policy

Rules available to build Policies:

Available Rules	Value
Classification Protection	Keep Group / Team owners from modifying native classifications
External Sharing Settings	Govern Guest Access for individual Teams and Groups
Membership / Ownership Restriction	Whitelist / Blacklist users by name or AD properties (role, title, geography, dept, etc.)
Outlook Group Visibility	Controlling visibility of Groups / Teams upon creation to flag violations
Membership / Ownership Size	Cap the size of Members / Owners by a specific number, preventing top-heavy groups
Privacy Restriction	Prevent Groups / Teams from switching from Private to Public teams, affecting visibility
Access Request Settings	For SharePoint / OneDrive to enforce how permissions are processed
Deletion Restriction	Control SharePoint (libraries, sites) deletions to create a safer work environment
Permission Inheritance	Monitor for broken inheritance and standardize how information is shared
External User Scans	Identify external user access to SharePoint and OneDrive content
Site External Sharing Settings	Control the SharePoint and OneDrive external sharing settings for each site



Monitor what's
important



Easily monitor user activity, permissions, and sensitive content.

Prioritize security
issues with ease



Take action where it matters most, optimizing efficiency and business impact.

Automate
Policy enforcement



Reduce oversight burden with quick, decisive, automated actions in near real time.

Prove Your
Outcomes



Prove adoption and risk reduction to your stakeholders and organization.



More resources:

[See PI In action! How to videos available here...](#)

[Implementing a Best Practice Approach to Risk-Based Data Protection and Cybersecurity](#)

[Securing Collaboration: 5 Risk Management Challenges in Office 365](#)

[The difference between external access and guest access](#)

[Data Protection and Compliance Resources](#)





AvePoint's Newest Solution Protects Your O365 Data

**Determine who is accessing your
sensitive data and automate policies
with PI.**



Ron Delaney

Training and Development Manager,
AvePoint

In 30 minutes we will show you:



How PI extends the capabilities in the Microsoft Security and Compliance Center



How PI identifies and prioritizes risks like external users accessing sensitive data, shadow users, anonymous links, nested groups, and more



Common, granular policies that can be set up in minutes to mitigate these risks



and more!

