

Empower your remote workforce with data security in OneDrive & SharePoint

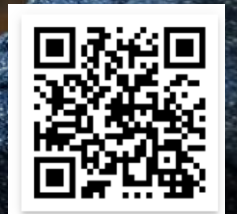


Sesha Mani

Principal Group Product Manager, Microsoft 365 Security and Compliance

[/in/seshamani](#)

[@SeshaManiS](#)



Nikita Bandyopadhyay

Senior Program Manager – Microsoft 365 Security and Compliance



Ankita Kirti

Product Marketing Manager – OneDrive



OneDrive

The intelligent files app for Microsoft 365



**View and capture all files
and photos from any
device**



**Share and work
together with anyone
in real-time**



**Organize and find files
that matter most across
the organization**

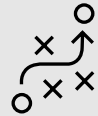


**Keep files backed up,
secured and protected**

Agenda



Trends shaping the
security landscape



Our **new security controls** to your
unique challenges



Our new
compliance controls to your
regulatory needs

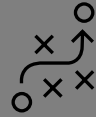


Roadmap - Q&A

Agenda



Trends shaping the
security landscape



Our **new security controls** to your
unique challenges



Our new
compliance controls to your
regulatory needs



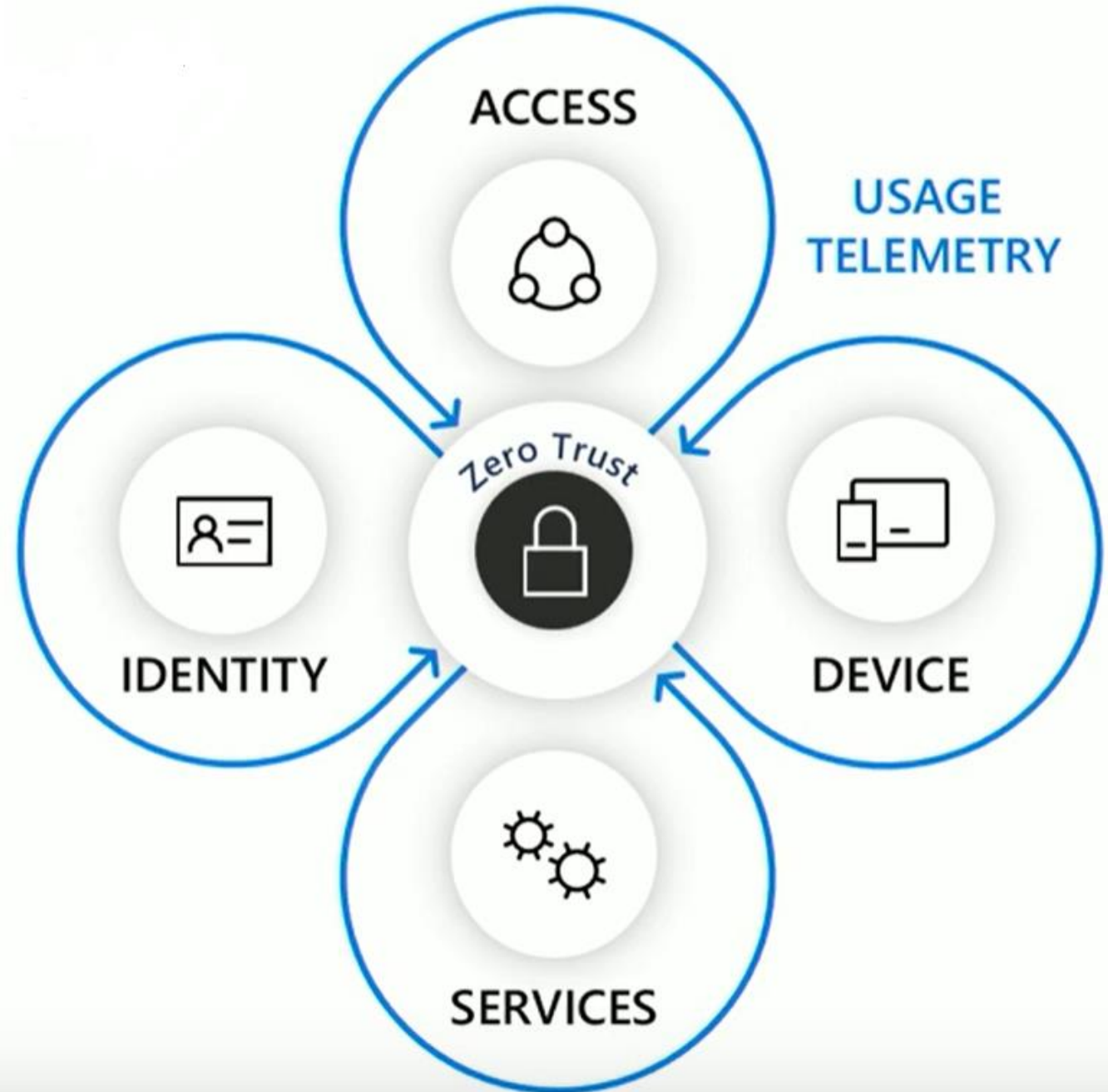
Roadmap - Q&A

Zero trust model

Strong user identity

Managed device

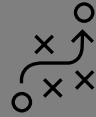
Least privileged access



Agenda



Trends shaping the
security landscape



Our **new security controls** to your
unique challenges



Our new
compliance controls to your
regulatory needs

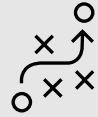


Roadmap - Q&A

Agenda



Trends shaping the
security landscape



Our new **security controls** to your
unique challenges

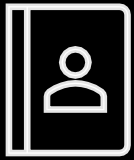


Our new
compliance controls to your
regulatory needs



Roadmap - Q&A

Security pivots and available controls



Users

Internal vs External
(Guests)

MFA Policy

Sharing policies



Devices

Mobile Device Mgt
(Intune)

Fine grain
Conditional access
(Unmanaged devices)

Idle session
timeout



Locations

IP Address Policy

AAD's CA Policy



Info Protection

Sensitivity labels for Files

Sensitivity labels for
Teams/Sites **

Auto classification **

** In public preview, others Generally available

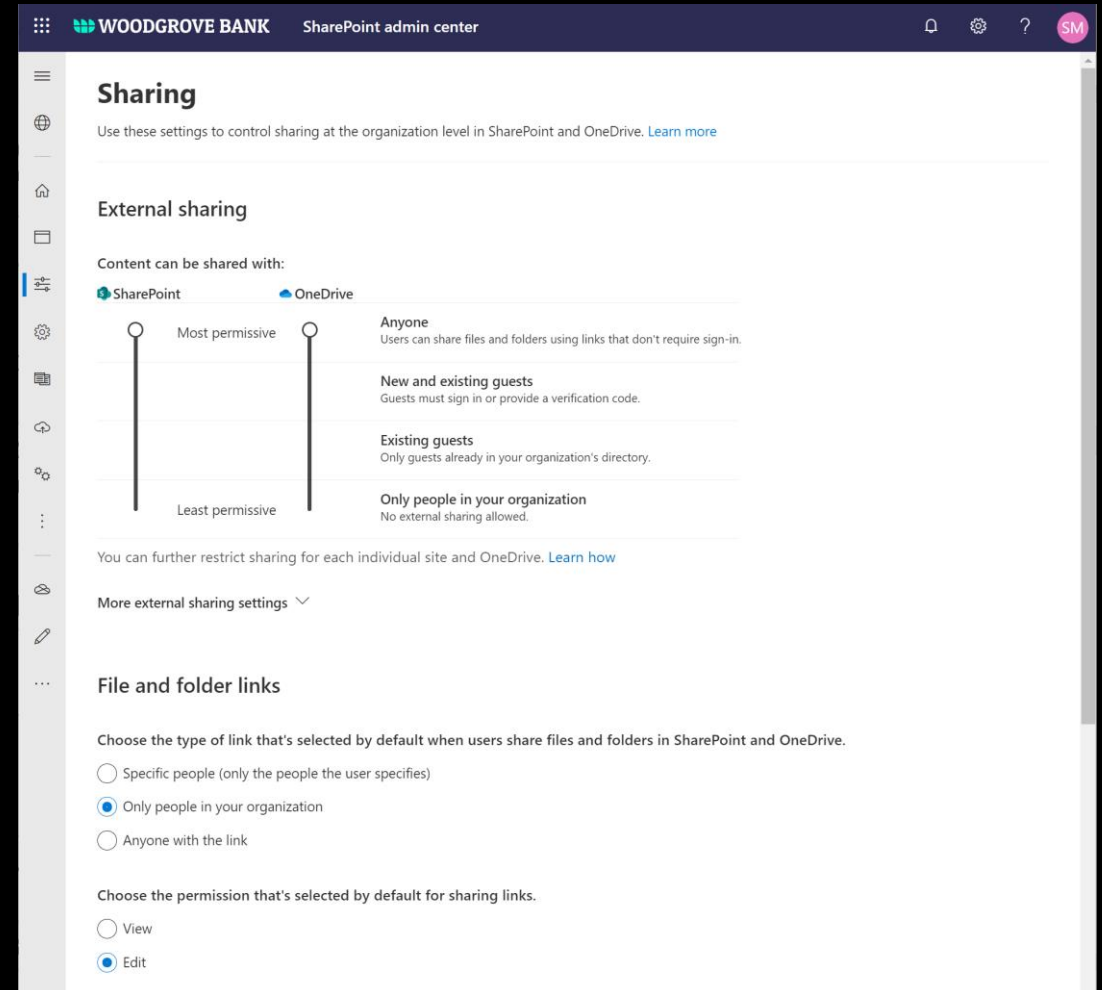
Users – Sharing and MFA access policies

Sharing

- Security spectrum of settings from Internal-only to Anyone links
- External sharing report
- Automatic expiration of external access

Conditional access

- Require all external guest users to authenticate with MFA (multi-factor-authentication)
- Granular conditional access policies – example provide limited access from unmanaged devices



The screenshot shows the SharePoint admin center interface for WOODGROVE BANK. The page is titled "Sharing" and provides settings for controlling sharing at the organization level. It includes sections for "External sharing" and "File and folder links".

Sharing
Use these settings to control sharing at the organization level in SharePoint and OneDrive. [Learn more](#)

External sharing
Content can be shared with:

SharePoint OneDrive

Most permissive Least 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.
- 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

Demo

Sharing policies

**Granular conditional
access policies**



Simplify info protection using Sensitivity Labels

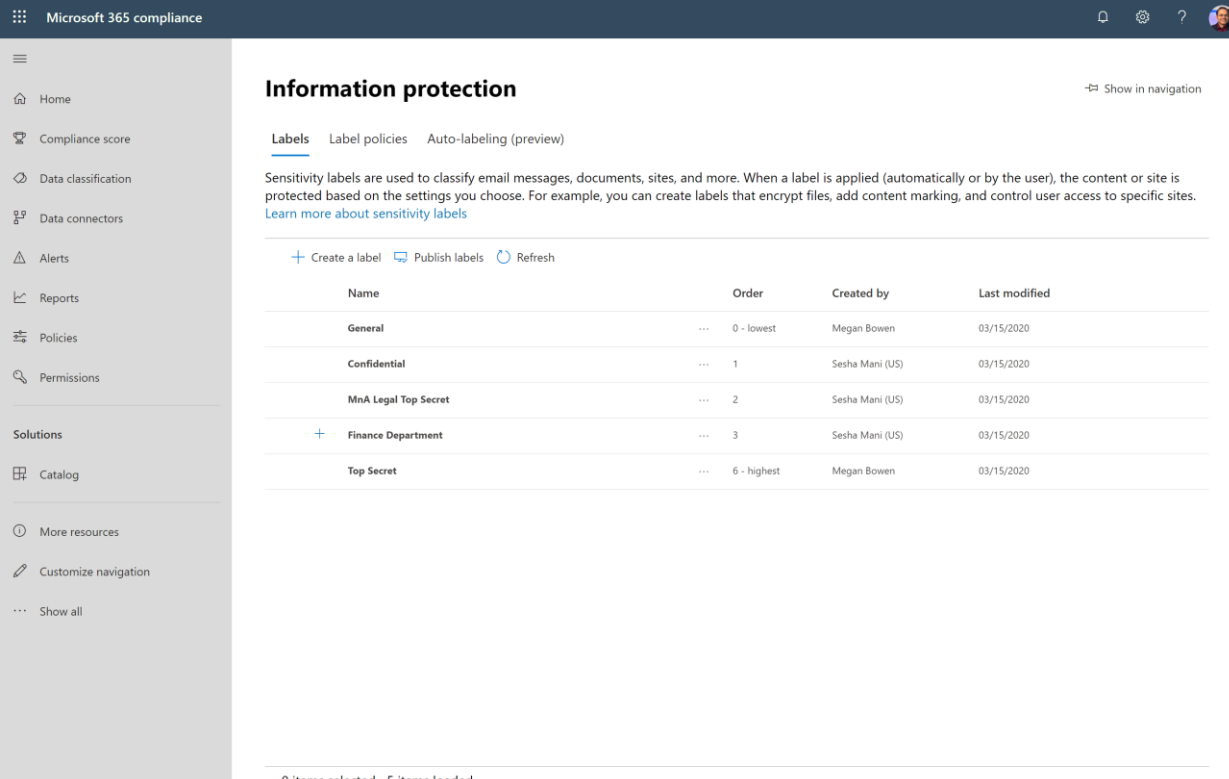
MIP (Microsoft Information Protection)

Easily classify, detect, and label your ever-increasing digital data

Associate labels with security and access policies

Set consistent policies on Files, Sites, Teams and Microsoft 365 Groups

Unified Labels across M365



The screenshot displays the Microsoft 365 compliance center interface. The left sidebar contains navigation options: Home, Compliance score, Data classification, Data connectors, Alerts, Reports, Policies, Permissions, Solutions, Catalog, More resources, Customize navigation, and Show all. The main content area is titled "Information protection" and includes sub-sections for Labels, Label policies, and Auto-labeling (preview). A descriptive paragraph explains that sensitivity labels are used to classify content and protect it based on settings. Below this is a table of existing labels.

Name	Order	Created by	Last modified
General	0 - lowest	Megan Bowen	03/15/2020
Confidential	1	Sesha Mani (US)	03/15/2020
MnA Legal Top Secret	2	Sesha Mani (US)	03/15/2020
+ Finance Department	3	Sesha Mani (US)	03/15/2020
Top Secret	6 - highest	Megan Bowen	03/15/2020

0 items selected. 5 items loaded.

Simplify info protection – Auto Classification with Sensitivity Labels

Even if users forget/neglect labelling your sensitive data is protected

Over 100 sensitive info types to create auto labelling policy

Policy simulation helps you test policies

Microsoft 365 compliance

Information protection

Labels Label policies Auto-labeling (preview)

Create auto-labeling policies to automatically apply sensitivity labels to email messages or files that contain sensitive info. To confirm that labels will be applied to the correct items, you'll first run policies simulation mode so you can review items that will be labeled when the policy is activated.

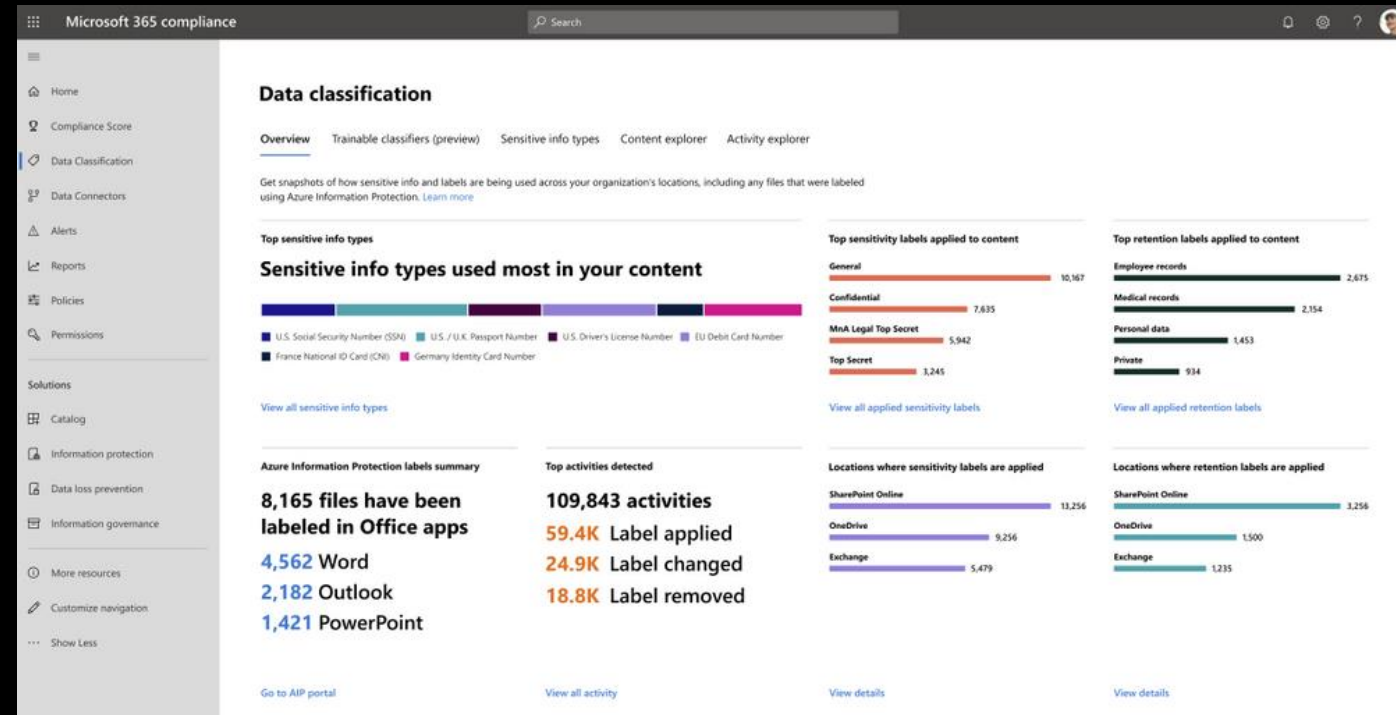
+ Create policy Refresh 3 items Search

Name	Locations	Date	Status	Label applied	Last modified
Simulation (2)					
Social Security	Exchange, SharePoint	05/14/2020	Simulation	Confidential	Sesha Mani
U.S. Financial Data in OneDrives	OneDrive for Business	05/14/2020	Simulation	Highly Confidential	Sesha Mani
On (1)					
U.S. Federal Trade Commission (FTC) Consumer Rules	SharePoint	03/17/2020	On	Highly Confidential	Sesha Mani

Labels analytics - 'Know your data' - leverage insights to govern

Data classification shows you full insights to how many items are labeled and in which service

O365 Audit logs shows detailed view of labels activities in the organization



Demo

**Sensitivity labels in Files
and Sites/Teams**

Auto classification

Labels analytics





**Would you like to try Sensitivity Labels in
SharePoint/OneDrive/Teams?**

Generally Available

Sensitivity Labels for Files with protection in SharePoint, OneDrive, and Teams

<https://aka.ms/M365FilesLabelsGA>



Generally Available

Sensitivity Labels for Teams, SharePoint Sites, and M365 Groups

<https://aka.ms/MIPsitesLabelsGA>



Generally Available

Auto Classification with Sensitivity Labels

<https://aka.ms/SPOAutoClassification>



But, wait there's more...



DLP – Data loss prevention policies in SharePoint and OneDrive

Block external access by default

Create consistent data loss prevention (DLP) rules across Office 365

Protect your content by treating it sensitive-by-default and prevent external sharing until a DLP (Data Loss Prevention) scan runs

For sensitive files block anonymous access

The screenshot displays the 'Edit rule' configuration window in the Microsoft 365 compliance center for Woodgrove Bank. The window is divided into three main sections: Exceptions, Action, and User notification.

- Exceptions:** A section titled 'Exceptions' with the text 'We won't apply this rule to content that matches any of these exceptions.' It includes a '+ Add exception' button.
- Action:** A section titled 'Action' with the text 'Use actions to protect content when the conditions are met.' It contains a sub-section 'Restrict access or encrypt the content' with a trash icon. Under this sub-section, the 'Restrict access or encrypt the content' option is selected with a blue checkmark. Below it, three radio button options are listed:
 - Block people from sharing and restrict access to shared content. This option includes the text 'Block these people from accessing SharePoint, OneDrive, and Teams content' and three radio button sub-options:
 - Everyone, Only the content owner, the last modifier and the site admin will continue to have access.
 - Only people outside your organization, people inside your organization will continue to have access.
 - Only people who were given access to the content through the "Anyone with the link" option.

- User notification:** A section titled 'User notification' with the text 'Use Notifications to inform your users and help educate them on the proper use of sensitive info'. It features a toggle switch set to 'On'. Below this, a note states 'Please note: Notifications for Teams will be displayed in the chat client itself.' Under 'Email notifications', two radio button options are present:
- Notify the user who sent, shared, or last modified the content.
- Notify these people: This option includes three checked checkboxes:
 - The person who sent, shared, or modified the content
 - Owner of the SharePoint site or OneDrive account
 - Owner of the SharePoint or OneDrive content

At the bottom of the window, there are buttons for 'Save' and 'Cancel', along with a link for 'Add or remove people' and checkboxes for 'Customize the email text' and 'Customize the email subject'.

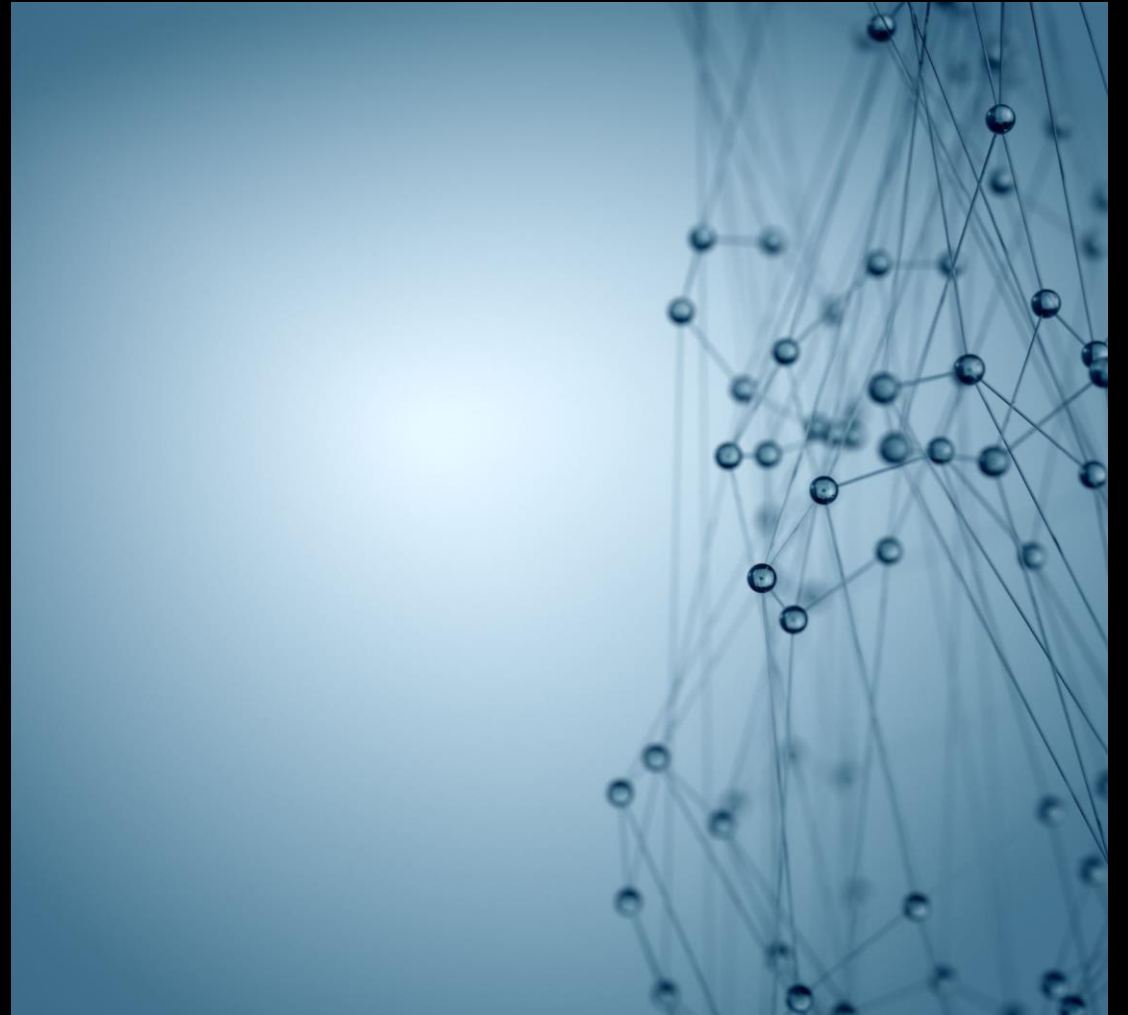
Demo – Data loss prevention (DLP)

Sesha Mani



Recap – new security controls

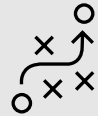
1. Sensitivity Labels with Protection – Search experience for encrypted files
2. Classify your sites/teams using Sensitivity Labels
3. Auto Classification with Sensitivity Labels
4. Labels Analytics & Auditing
5. DLP Block external access by default



Agenda



Trends shaping the
security landscape



Our new **security controls** to your
unique challenges



Our new
compliance controls

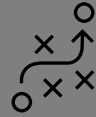


Roadmap - Q&A

Agenda



Trends shaping the
security landscape



Our new **security controls** to your
unique challenges



Our new
compliance controls



Roadmap - Q&A

New compliance controls

1. Multi-geo
2. Insider risk management
3. Information barriers
4. Retention labels
5. eDiscovery
6. Audit/Alerts

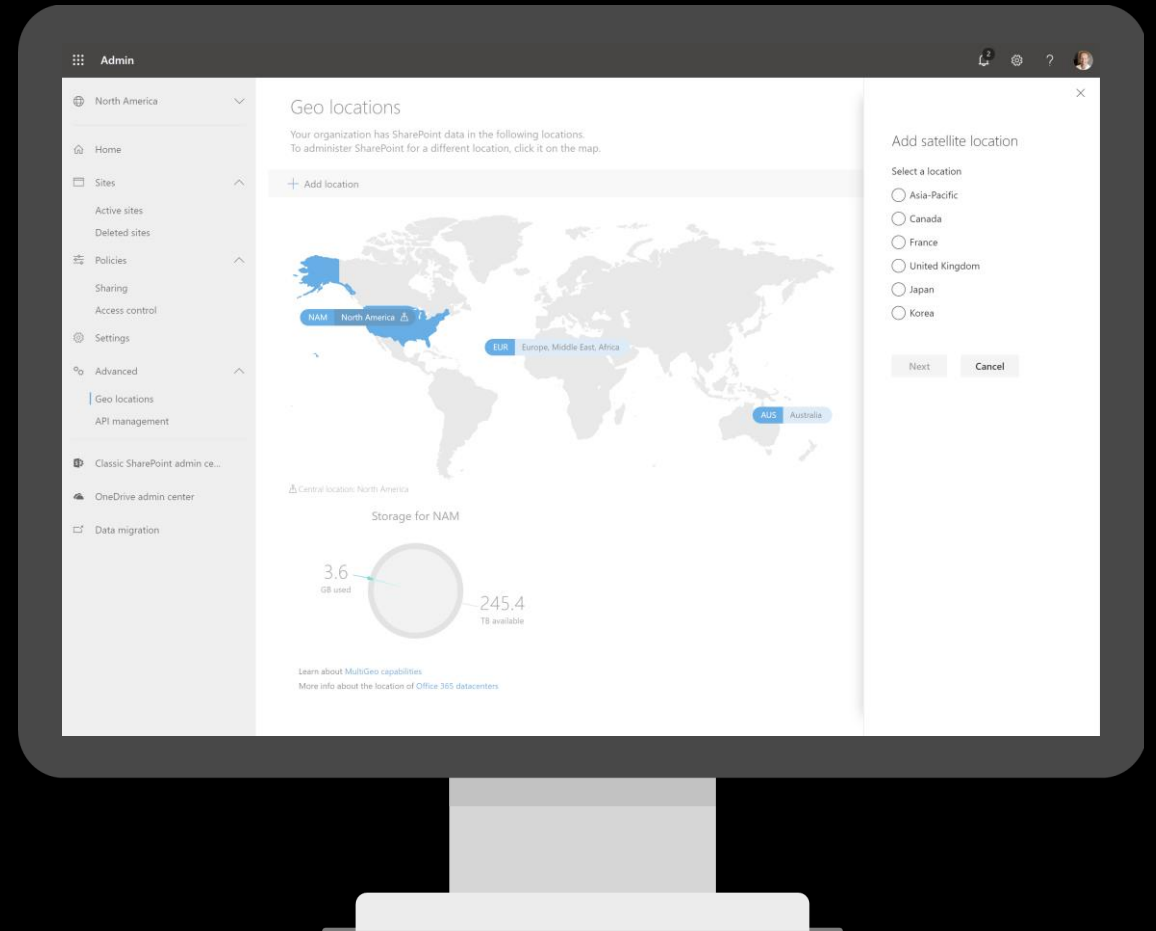


Stay ahead of compliance changes – Multi-Geo

Meet compliance obligations for data residency with OneDrive and SharePoint multi-geo capabilities – Now minimum seats criteria is only 250

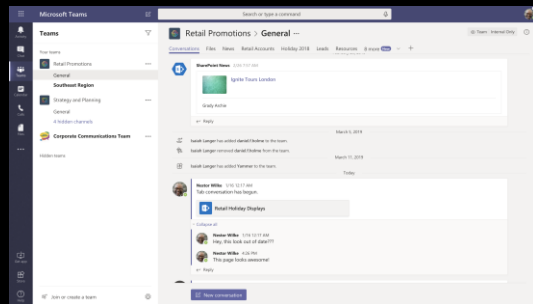
Meet your **GDPR** needs with built-in tools

<http://aka.ms/SPOMultigeo>



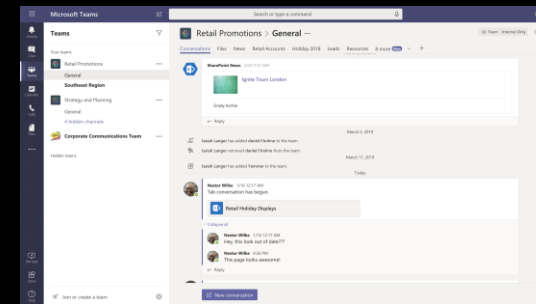
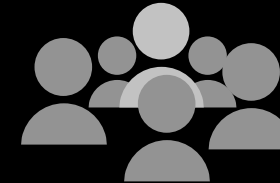
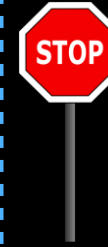
Investment Banking Information

Conditional Access:
IB Must Match
Members only



Advisory Information

Conditional Access:
IB Must Match
Members only



Information barriers (IB)

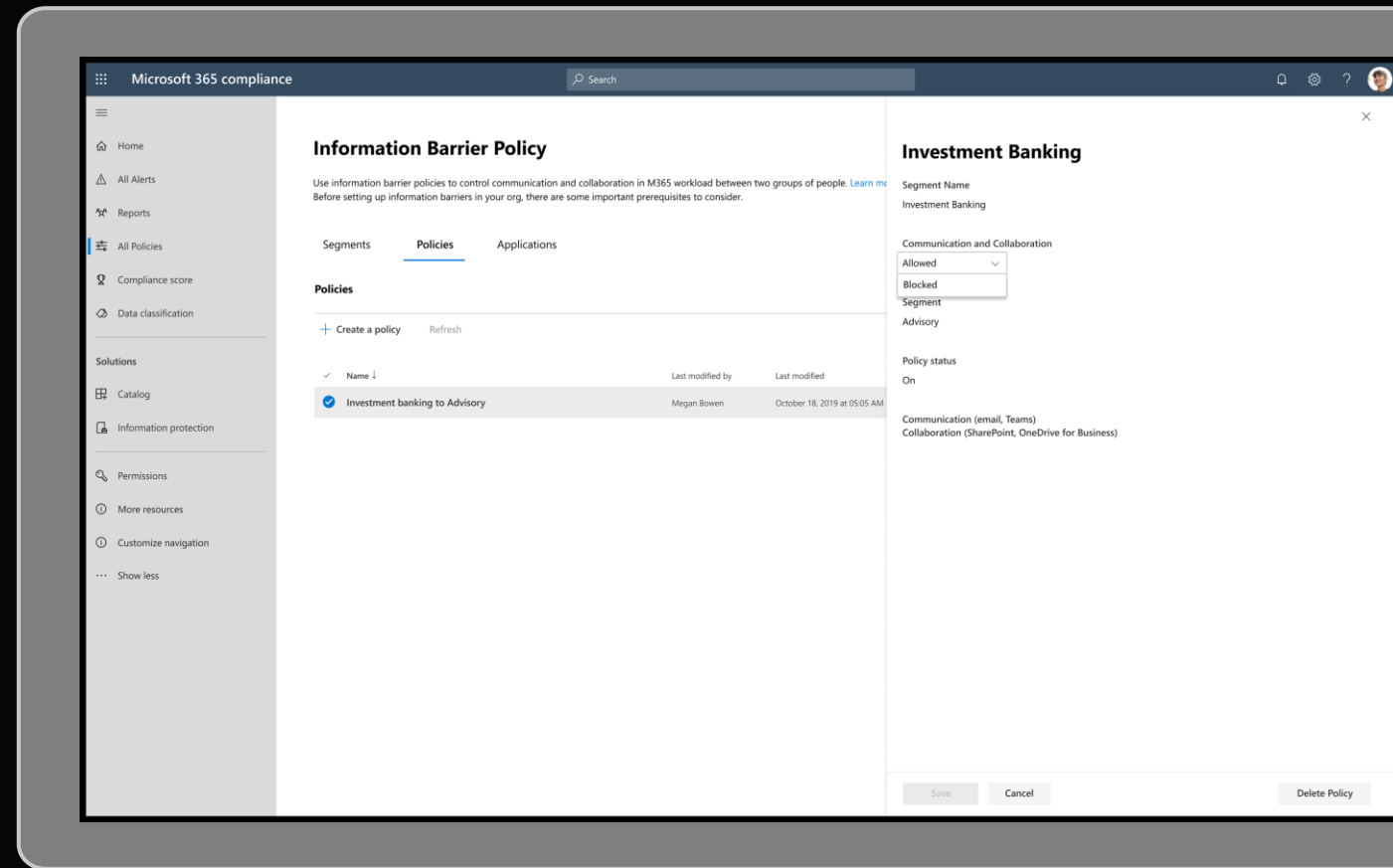
Segment users and define policy per your compliance needs

Segment users and create policy
per regulatory and compliance needs

OneDrive automatically honors user's IB
policy

Associate segments to SharePoint site

Sample scenario: FINRA Compliance
requirement in Financial sector



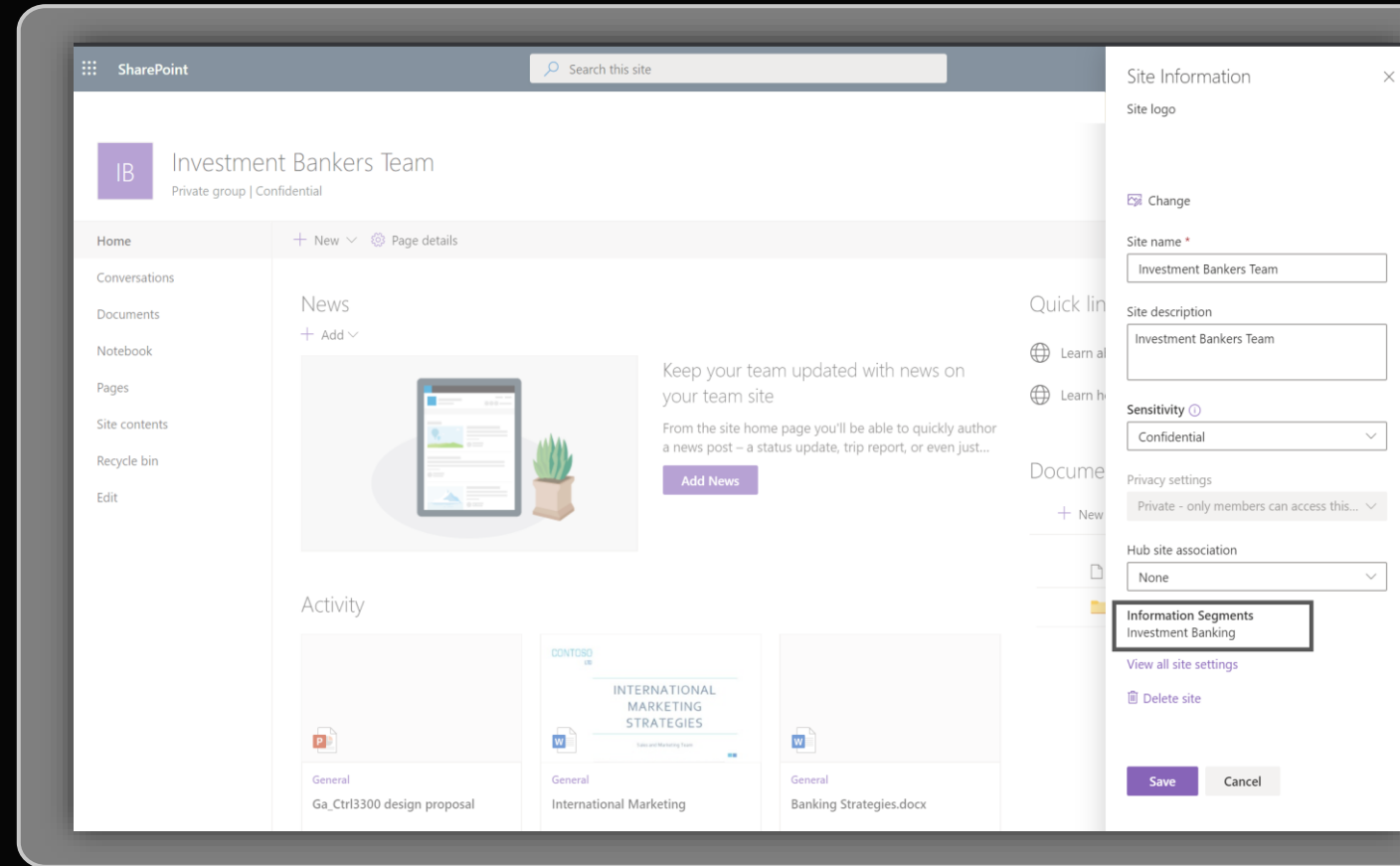
Information barriers (IB)

Segment users and define policy per your compliance needs

Access control per site's segments

Sharing control per site's segments

Add members per site's segments



* Currently, only the contents of the site are segment associated.
All other group resources are currently not segment associated.

Recap – Information Barriers (IB)

- E5 Comprehensive compliance feature
- One place M365 Compliance Center to create IB Segments & Policies
- SharePoint and OneDrive supports IB

<https://aka.ms/SPOInfobarriers>

<https://aka.ms/OneDriveInfobarriers>

Insider Risk Management

Identify and take action on critical insider threats

Rich Insights via tailored templates

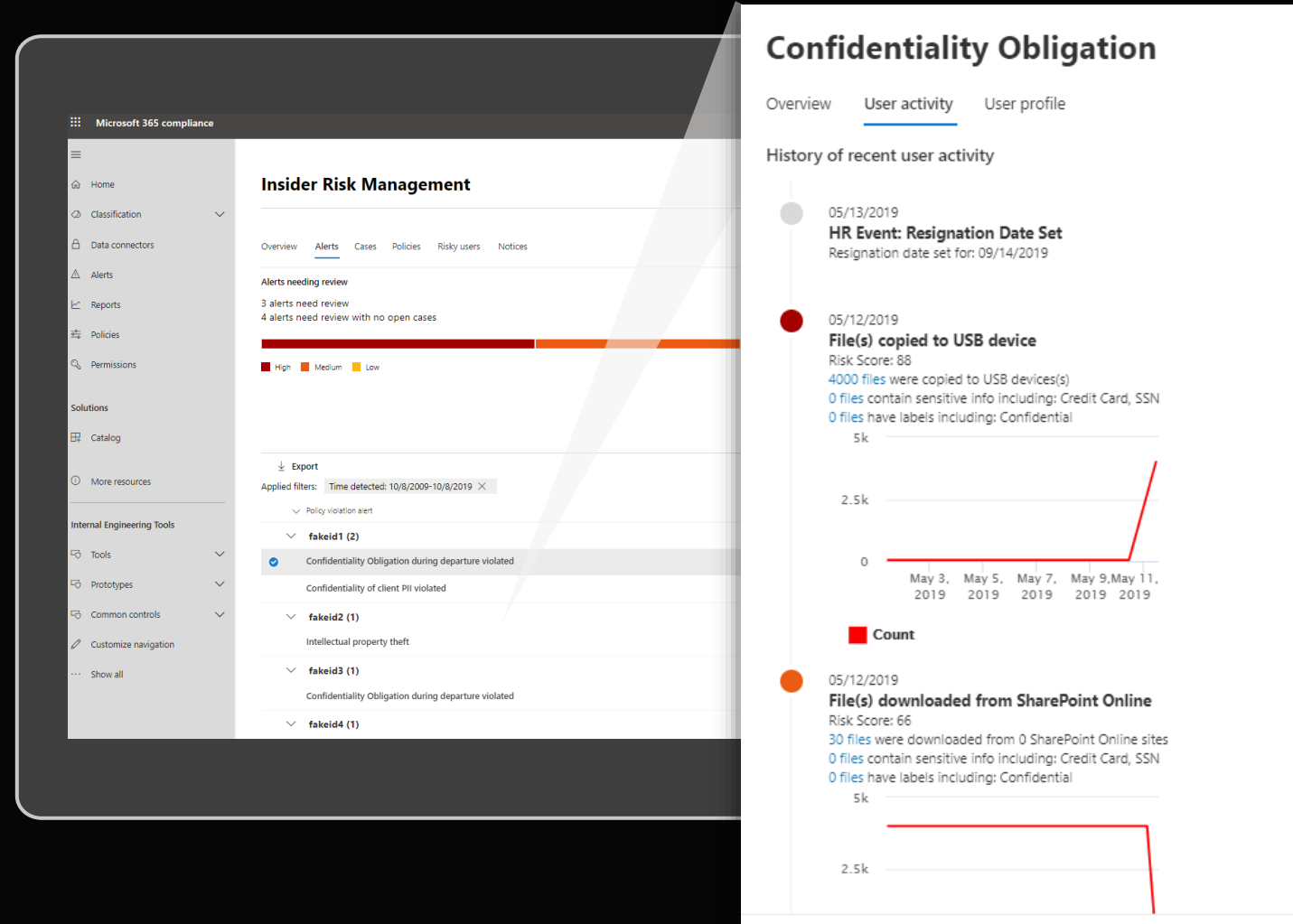
Machine learning correlates native¹ and third-party signals to identify insider risks

Privacy built-in

Anonymity controls ensure data about risks is appropriately managed

End-to-end investigations

Integrated investigation workflows allow for collaboration across IT, HR and legal



1. Teams, SharePoint Online, Exchange Online, OneDrive for Business and Windows 10

Retention labels

Identify and take action on content to comply with regulatory needs and internal policies

Create labels

To meet your regulatory needs and policies

Manual labels

Exchange, SharePoint, OneDrive, Microsoft 365 groups

Auto-apply labels

Exchange, SharePoint, OneDrive, Microsoft 365 groups

The screenshot displays the 'Office 365 Security & Compliance' interface for 'WOODGROVE BANK'. It features a table of retention labels and a detailed view for the 'Product Retired' label.

<input type="checkbox"/>	Name	Created by
<input type="checkbox"/>	Australian Finance Data	Sesha Mani (US)
<input type="checkbox"/>	Employee Records	Megan Bowen
<input type="checkbox"/>	Medical Records Retention Policy	Megan Bowen
<input type="checkbox"/>	Personal Financial PII	Megan Bowen
<input checked="" type="checkbox"/>	Product Retired	Megan Bowen
<input type="checkbox"/>	Public	Megan Bowen
<input type="checkbox"/>	Private	Megan Bowen
<input type="checkbox"/>	Financial Data	Sesha Mani (US)
<input type="checkbox"/>	Confidential	Megan Bowen
<input type="checkbox"/>	PII Retention Policy	Megan Bowen

Product Retired

[Edit label](#) [Publish label](#) [Auto-apply a label](#)
[Delete label](#) [Explore items](#)

Name
Product Retired

Description for admins [Edit](#)
This label is event driven. This label is applied to product content when a product is being retired.

Description for users [Edit](#)

File plan descriptors [Edit](#)

Retention [Edit](#)
10 years
Preserve, review and delete
Based on an event

Reviewers [Edit](#)
MeganB@Contosobankcorp.OnMicrosoft.com

eDiscovery

Identify, preserve, review and produce content for civil litigation

1. Create eDiscovery Case

2. Put eDiscovery holds

3. Search relevant content

4. Export and download results

The screenshot shows the eDiscovery interface in the Office 365 Security & Compliance center for Woodgrove Bank. The left navigation pane includes options like Classification, Data loss prevention, Records management, Information governance, Supervision, Threat management, Mail flow, Data privacy, Search, eDiscovery, and Advanced eDiscovery. The main content area displays the eDiscovery page with a breadcrumb 'Home > eDiscovery', a description of the feature, and a table of active cases.

	Case name	Status	Created
Open	122456	Active	2019-05-19 11:42:25
Open	Legal Hold for US Banking	Active	2019-05-14 18:44:46
Open	Legal Hold for Banking Lit EUR	Active	2019-05-14 18:27:39
Open	Legal Hold for Banking Litigation	Active	2019-05-13 15:36:33

Audit & Alerts

Unified audit search and alert for site activities

Search site activities

Create Alerts

Home > Audit log search

Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. [Learn more about searching the audit log](#)

Search Clear **Results** 12 results found Filter results Export results

Activities

Shared file, folder, or site

Start date

2020-05-01 00:00

End date

2020-05-29 00:00

Users

Show results for all users

File, folder, or site

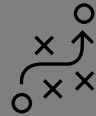
Add all or part of a file name, folder name, or URL

Date	IP address	User	Activity	Item	Detail
2020-05-28 15:09:01		sesha@contosobankcorp.onmicr...	Shared file, folder, or site	https://contosobankcorp.sharep...	Shared with "Limited Access Sys...
2020-05-27 08:04:22	216.9.30.179	nikita@contosobankcorp.onmicr...	Shared file, folder, or site	https://contosobankcorp.sharep...	Shared with "Advisory Team Site...
2020-05-15 18:48:36	73.59.107.50	sesha@contosobankcorp.onmicr...	Shared file, folder, or site	https://contosobankcorp.sharep...	Shared with "SharingLinks.684d...
2020-05-15 18:48:36		sesha@contosobankcorp.onmicr...	Shared file, folder, or site	https://contosobankcorp.sharep...	Shared with "Limited Access Sys...
2020-05-12 23:42:00	50.35.77.126	sesha@contosobankcorp.onmicr...	Shared file, folder, or site	https://contosobankcorp.sharep...	Shared with "SharingLinks.9a7e...
2020-05-12 23:42:00		sesha@contosobankcorp.onmicr...	Shared file, folder, or site	https://contosobankcorp.sharep...	Shared with "Limited Access Sys...
2020-05-02 17:42:00	73.59.107.50	sesha@contosobankcorp.onmicr...	Shared file, folder, or site	https://contosobankcorp.sharep...	Shared with "SharingLinks.3767...
2020-05-02 17:42:00		sesha@contosobankcorp.onmicr...	Shared file, folder, or site	https://contosobankcorp.sharep...	Shared with "Limited Access Sys...
2020-05-02 16:57:06	73.59.107.50	sesha@contosobankcorp.onmicr...	Shared file, folder, or site	https://contosobankcorp.sharep...	Shared with "SharingLinks.76da...
2020-05-02 12:23:54		sesha@contosobankcorp.onmicr...	Shared file, folder, or site	https://contosobankcorp.sharep...	Shared with "Limited Access Sys...
2020-05-02 12:11:50		sesha@contosobankcorp.onmicr...	Shared file, folder, or site	https://contosobankcorp.sharep...	Shared with "Limited Access Sys...
2020-05-02 12:11:48	73.59.107.50	sesha@contosobankcorp.onmicr...	Shared file, folder, or site	https://contosobankcorp.sharep...	Shared with "SharingLinks.935a...

Agenda



Trends shaping the
security landscape



Our new **security controls** to your
unique challenges



Our new
compliance controls to your
regulatory needs

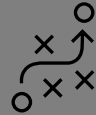


Roadmap - Q&A

Agenda



Trends shaping the
security landscape



Our new **security controls** to your
unique challenges



Our new
compliance controls












Roadmap - Q&A

Roadmap








Available Now thru Summer

-  Sensitivity Labels with Protection for Files (GA)
-  Auto Classification w/ Sensitivity Labels for Files (GA)
-  Sensitivity Labels for Teams/Sites (GA)
-  DLP Block external access by default for Files (GA)
-  DLP in Teams (GA)
-  M365 Multi-Geo Capabilities (GA)
-  M365 Insider risk management (GA)
-  Information Barriers IB (Preview, GA Summer)
-  Global reader role in SharePoint (GA)



EOY CY'2020

-  Office Rich Client Co-auth for Protected Files (Preview)
-  MFA Policy at Site Level (Preview)
-  Instant Session Revocation (Preview)
-  Expiring Permissions (GA)
-  DLP block anonymous access for sensitive files (GA)

Thank you!

Please join us for an AMA at <https://aka.ms/OneDriveAMA>

Get the latest technical documentation and guidance

<https://docs.microsoft.com/OneDrive>

Stay up to date on the latest product news

<https://aka.ms/OneDriveBlog>

Give us feedback and input on the roadmap

<https://OneDrive.UserVoice.com>

OneDrive user adoption resources:

<https://aka.ms/OneDriveAdoption>

OneDrive deployment quick reference:

<https://aka.ms/syncidealstate>

Subscribe to Sync Up – a OneDrive podcast

<https://aka.ms/SyncUp>