

Need to Know Microsoft 365 Webinar January 2025

@directorcia

<http://about.me/ciaops>

Web cast has started

Web cast is being recorded

If you can't hear anything check
your speaker settings

For questions after the event:

Email : director@ciaops.com

Twitter : [@directorcia](https://twitter.com/directorcia)

CIAOPS Academy

Login

Sign Up

Webinar recordings at:

Need to Know

Technology training

Enroll now

www.ciaopsacademy.com

Free access for CIAOPS patrons



Please:

- **Turn off your mobile**
- **Turn off your email**
- **Have somewhere to take notes**

Agenda

- Microsoft 365 Update
- Data Protection in Microsoft 365
- Q & A



Microsoft 365 Update

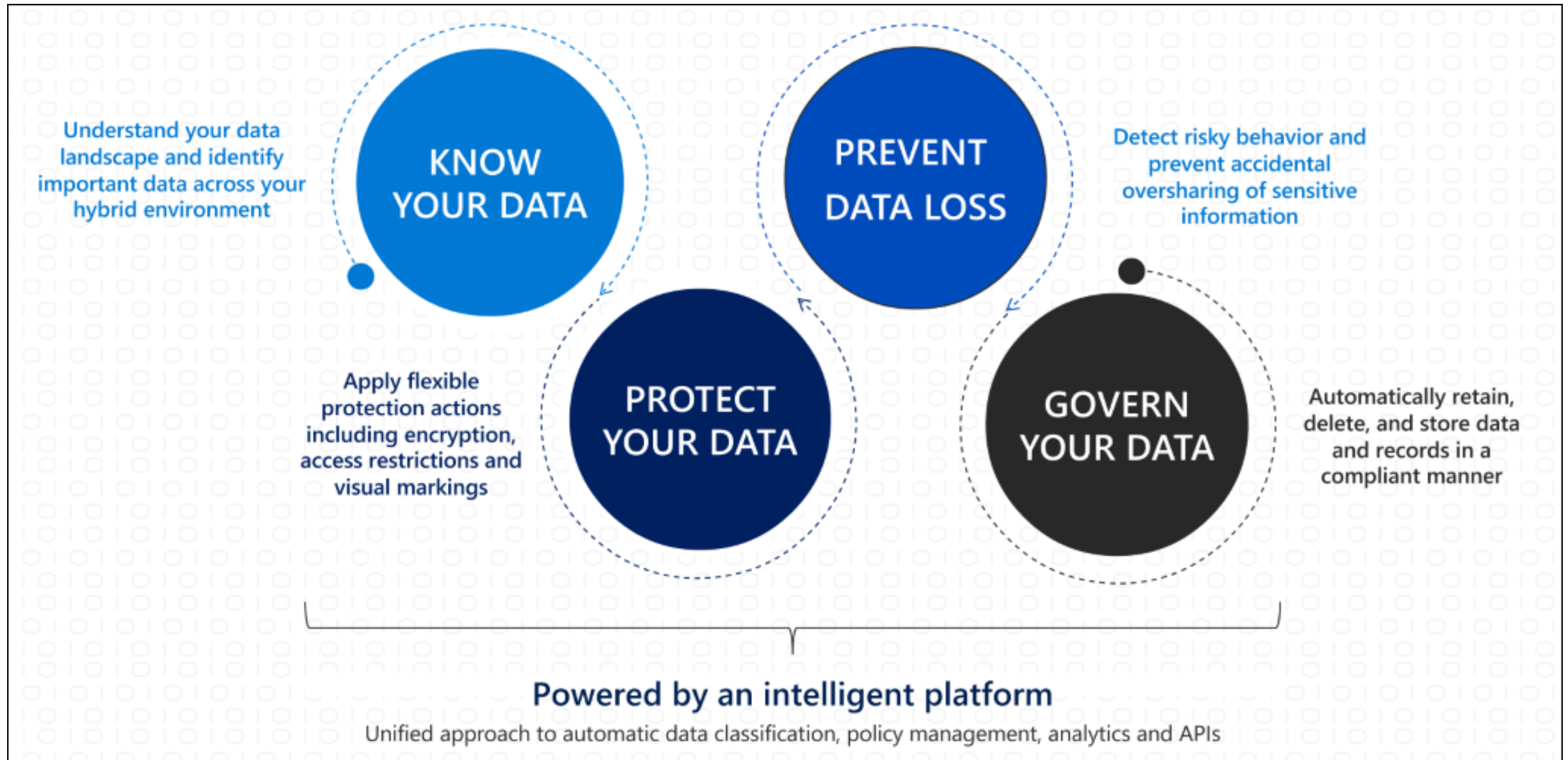
News

- MFA Mandatory for M365 administration portal
 - <https://techcommunity.microsoft.com/blog/microsoft365businessblog/announcing-mandatory-multifactor-authentication-for-the-microsoft-365-admin-cent/4369645>
- New Identity Secure Score recommendations in General Availability
 - <https://techcommunity.microsoft.com/blog/identity/new-identity-secure-score-recommendations-in-general-availability/4369133>
- Microsoft and OpenAI evolve partnership to drive the next phase of AI
 - <https://blogs.microsoft.com/blog/2025/01/21/microsoft-and-openai-evolve-partnership-to-drive-the-next-phase-of-ai/>
- Windows 11 Security Book
 - <https://learn.microsoft.com/en-us/windows/security/book/>
- Enhancing Security with Entra PIM and Conditional Access Policy using Authentication Context
 - <https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/enhancing-security-with-entra-pim-and-conditional-access-policy-using-authentica/4368002>

Data Protection in Microsoft 365

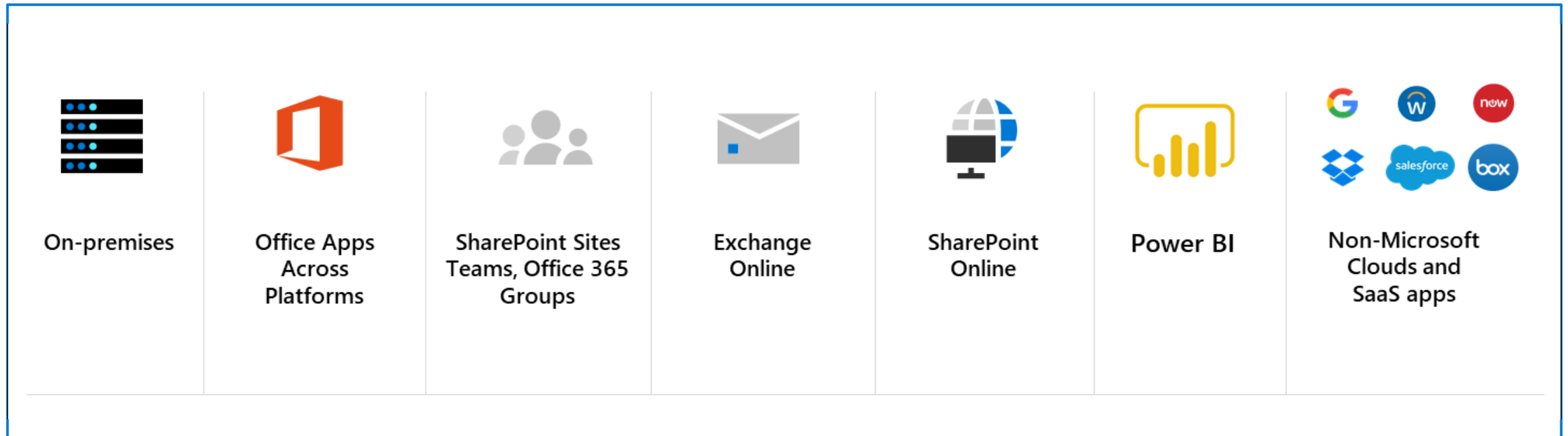


Introduction to information protection



Protect your data

Information protection is integrated into Microsoft 365 apps and services like:



Introduction to Microsoft 365 encryption

What is encryption in Microsoft 365?

- Encoding plain text into cipher text.
- Decryption requires encryption keys.
- Control access to authorized users or machines only.
- Differentiation between 'data at rest' and 'data in transit'

Data at rest

- Files saved on computers and mobile devices
- Documents and files saved in SharePoint Online and OneDrive
- Mails saved in Mailboxes in Exchange Online

Data in transit

- Documents and files accessed in SharePoint Online and OneDrive
- Mails transported between servers
- Shared files and conversations in Teams meetings

Data permissions

BROWSE

PERMISSIONS

Delete unique permissions

Inheritance

Grant Permissions

Grant

Edit User Permissions

Modify

Remove User Permissions

Modify

Check Permissions

Check

Home

Notebook

Documents

Recent

Calendar

SharePoint Online Permission Report

Site Contents

EDIT LINKS

Some items of this list may have unique permissions which are not controlled from this page. [Show these items.](#)

There are limited access users on this site. Users may have limited access if an item or document under the site has been shared with them. [Show users.](#)

This library has unique permissions.

<input type="checkbox"/>	<input type="checkbox"/>	Name	Type	Permission Levels
<input type="checkbox"/>	<input type="checkbox"/>	Approvers	SharePoint Group	Approve
<input type="checkbox"/>	<input type="checkbox"/>	Designers	SharePoint Group	Design
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Excel Services Viewers	SharePoint Group	View Only
<input type="checkbox"/>	<input type="checkbox"/>	Hierarchy Managers	SharePoint Group	Manage Hierarchy
<input type="checkbox"/>	<input type="checkbox"/>	Records Center Web Service Submitters for records	SharePoint Group	Records Center Web Service Submitters
<input type="checkbox"/>	<input type="checkbox"/>	Restricted Readers	SharePoint Group	Restricted Read

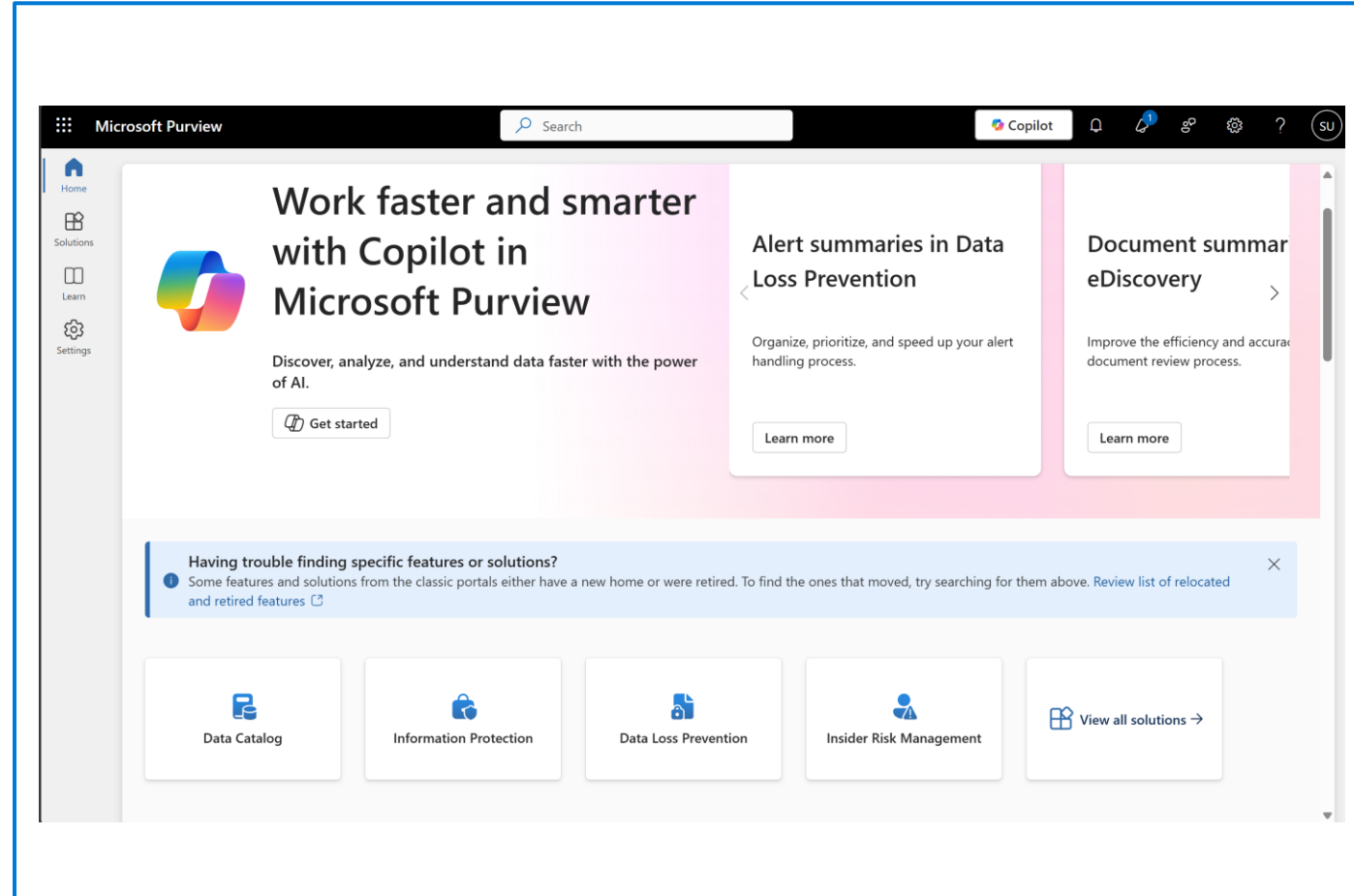
Microsoft Purview compliance portal

Microsoft Purview compliance portal

- A view of how the organization is meeting its compliance requirements.
- Solutions that can be used to help with compliance.
- Information about active alerts.
- And more...

Navigation

- Access to alerts, reports, policies, compliance solutions, and more.
- Add or remove options for a customized navigation pane.
- Customize navigation control.



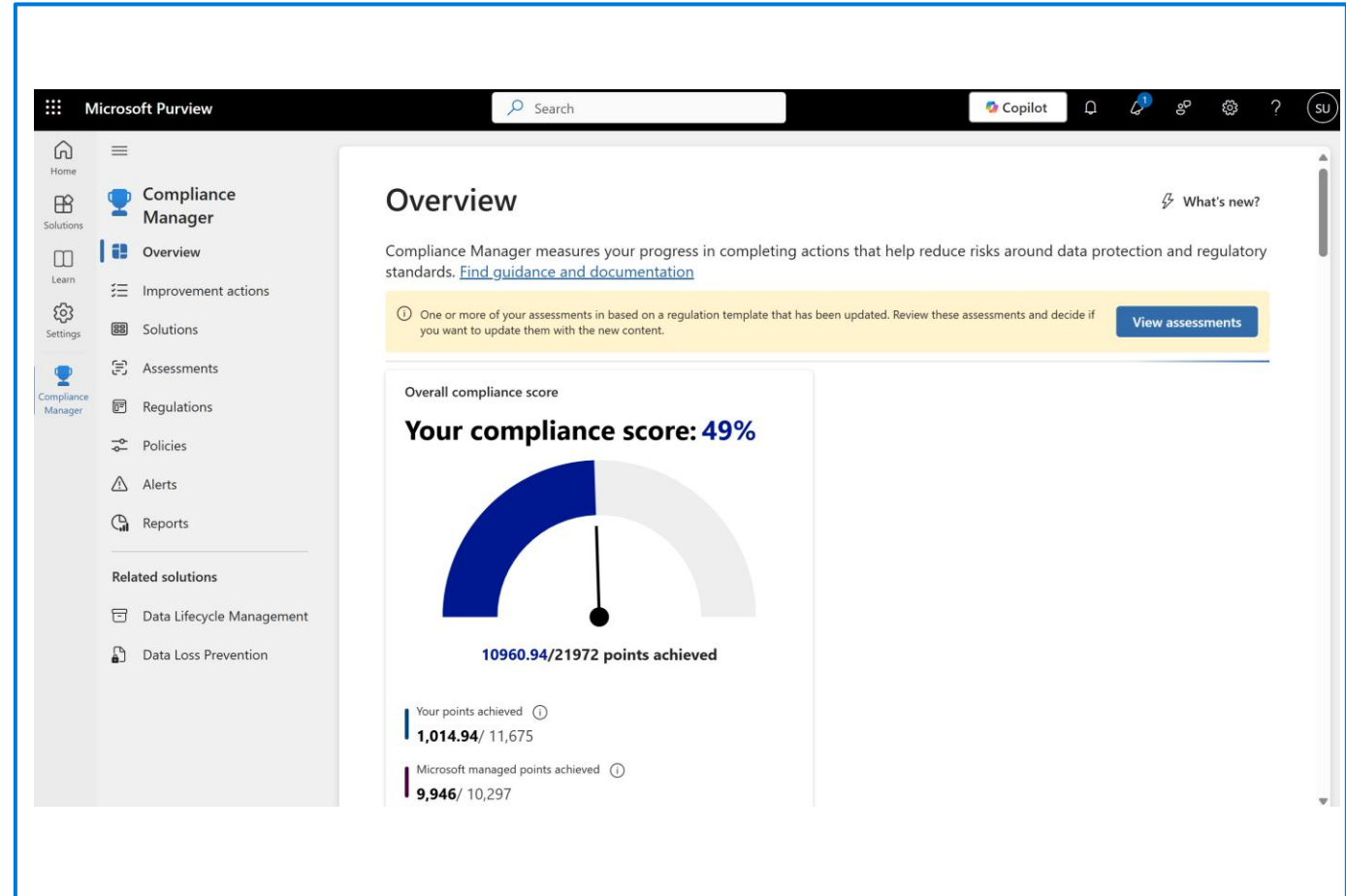
Compliance Manager

Compliance Manager simplifies compliance and reduces risk by providing:

- Prebuilt assessments based on common standards
- Workflow capabilities to complete risk assessments
- Step-by-step improvement actions
- Compliance score, shows overall compliance posture

Key elements of Compliance Manager

- Controls
- Assessments
- Templates
- Improvement actions



Data classification capabilities of the compliance portal



Sensitive information types.



Trainable classifiers: Pre-trained classifiers and Custom trainable classifiers.



Understand and explore the data.



The content explorer: It enables administrators to gain visibility into the content that has been summarized in the overview pane.



The activity explorer: It can monitor what's being done with labeled content across the organization.

Classify data using sensitive information types

Information protection and governance solutions and where in those solutions you can use sensitive information types:



Information protection: Sensitivity label auto-labeling policies



Data loss prevention (DLP): DLP policies



Data Lifecycle Management: Retention policies and retention label auto-apply policies



Records management: Retention label auto-apply policies

Solutions

[Explore all →](#)



Audit



Communication Compliance



Compliance alerts



Compliance Manager



Data Catalog



Data Lifecycle Management



Data Loss Prevention



Data Security Posture Management (preview)



DSPM for AI



eDiscovery



Information Barriers



Information Protection



Insider Risk Management



Records Management

DEMO

Sensitivity labels and policies

Sensitivity labels

Labels are:

- Customizable
- Clear text
- Persistent

Usage:

- Encrypt email and documents.
- Mark the content.
- Apply the label automatically.
- Protect content in containers: sites and groups.
- Extend sensitivity labels to third-party apps and services.
- Classify content without using any protection settings.

Label policies

Policies enable admins to:

- Choose the users and groups that can see labels.
- Apply a default label to all new emails and documents.
- Require justifications for label changes.
- Require users to apply a label (mandatory labeling).
- Link users to custom help pages.

Once a sensitivity label is applied to an email or document, any configured protection settings for that label are enforced on the content.

Apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, and SharePoint sites

- Labels may be published for use in Microsoft 365 Groups, Microsoft Teams, Yammer communities and SharePoint sites.
- You must activate labels in the tenant level via the Azure AD PowerShell module before they can be used.
- Sensitivity labels can be manually assigned to SharePoint Sites and Teams sites through the creation settings.
- Labels can be changed through the properties of existing SharePoint sites or Microsoft Teams.
- A sensitivity label is applied to a Group in the Azure portal through Azure services > Groups > properties.

Retention labels and policies

Retention settings work with SharePoint, OneDrive, Teams, Yammer and Exchange and help organizations manage and govern information by ensuring content is kept only for a required time, and then permanently deleted.

Retention labels:

- Are applied at an item level.
- Emails and documents can have only a single retention label assigned to it at a time.
- Retention settings from retention labels travel with the content in your Microsoft 365 tenant.
- Can be applied manually or automatically.
- Retention labels support disposition review of the content before it's permanently deleted.

Retention policies:

- Are applied at site or mailbox level.
- Can be applied to multiple locations or specific locations or users.
- Items inherit the retention settings from their container.
- If an item is moved, the retention setting does not travel to the new location.

DEMO

Data loss prevention overview

Each DLP policy contains:

Where to protect the content

Content is protected in locations like SharePoint Online, Exchange Online, OneDrive accounts, Microsoft Teams chat and channel messages, and Windows 10 or higher devices.

When and how to protect the content

When and how to protect the content is defined by enforcing rules. A policy contains one or more rules, and each rule consists of conditions and actions at a minimum.



Identify content to protect

Use the following to identify content:

Content explorer

Content explorer identifies the email and documents in your organization that contain sensitive information.

Activity explorer

Activity explorer includes information on activity related to content that contains sensitive information, which can also inform what should be protected by DLP policies.

Data loss prevention

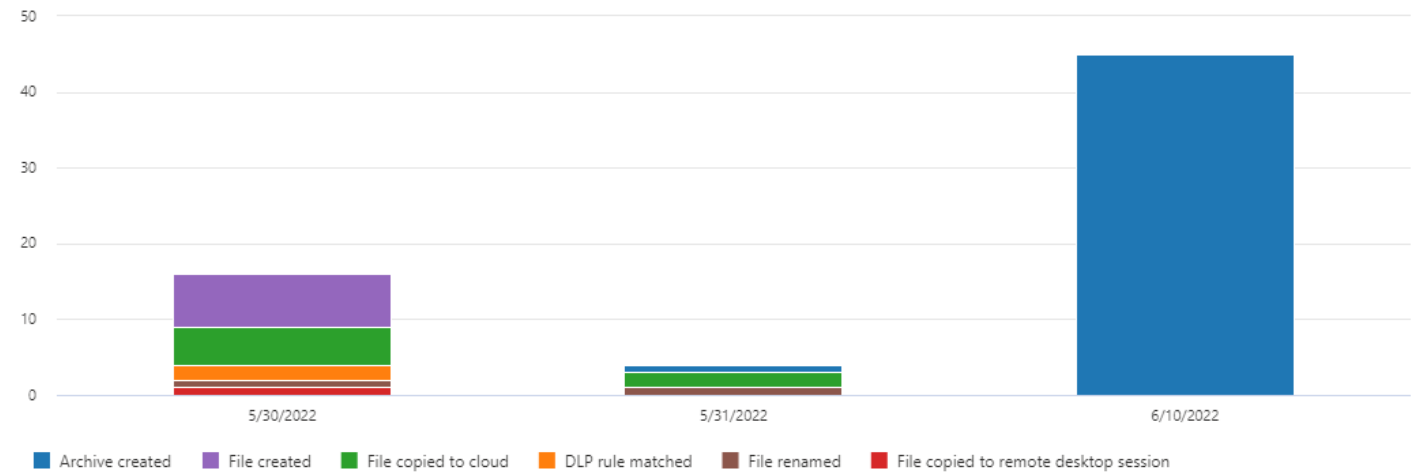
[Remove from navigation](#)

Overview Policies Alerts Endpoint DLP settings **Activity explorer**

Review activity related to content that contains sensitive info or has labels applied, such as what labels were changed, files were modified, and more. Label activity is monitored across Exchange, SharePoint, OneDrive, and endpoint devices. Support for more locations is coming soon. [Learn more](#)

Built-in filters [Reset](#) [Filters](#)

Date: 5/29/2022-6/10/2022 Activity: Any Location: Any User: Any Sensitivity label: Any



[Export](#) [Refresh](#)

65 items [Customize columns](#)

Define policy settings for your DLP policy

To create a DLP policy go to the **Microsoft Purview Portal**

Data loss prevention policy configuration



Choose the information to protect

DLP policy templates consist of one or more sensitive info types grouped into categories:

- **Enhanced**
- **Financial**
- **Medical and health**
- **Privacy**
- **Custom**

The screenshot shows the 'Choose the information to protect' step of the DLP policy creation process. On the left is a vertical progress bar with six steps: 'Choose the information to protect' (selected), 'Name your policy', 'Locations to apply the policy', 'Policy settings', 'Test or turn on the policy', and 'Review your settings'. The main content area is titled 'Start with a template or create a custom policy'. It includes a paragraph explaining that users can choose an industry regulation or create a custom policy. Below this are two informational messages: one stating that enhanced templates are not supported for on-premises file repositories and Power BI (preview), and another encouraging users to check out new enhanced policy templates that detect named entities. There is a search bar labeled 'Search for specific templates' and a dropdown menu currently set to 'All countries or regions'. At the bottom, under the heading 'Categories', there is a list of five categories: 'Enhanced' (with a shield icon), 'Financial' (with a document icon), 'Medical and health' (with a heart icon), 'Privacy' (with a person icon), and 'Custom' (with a pencil icon).

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](#)

Enhanced templates currently aren't supported for following location(s): On-premises file repositories, Power BI (preview)

Check out our new enhanced policy templates. These enhanced templates extend several of the original templates by also detecting named entities (such as full names and physical addresses). Just look for the templates labeled 'Enhanced' to start protecting even more personal data.

Search for specific templates

All countries or regions

Categories

- Enhanced
- Financial
- Medical and health
- Privacy
- Custom

Choose locations to apply the policy

Locations are places or service the DLP policy will apply to:









- **Exchange Online email**
- **SharePoint Online sites**
- **OneDrive accounts**
- **Microsoft Teams chat and channel messages**
- **Devices**
- **Microsoft Defender for Cloud Apps**
- **On-premises repositories**
- **Power BI (preview)**

Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

① Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. [Learn more about the prerequisites](#)

① At this time, protecting content in the following location isn't supported for enhanced DLP templates: On-premises file repositories. Either turn this location off or go back and choose a non-enhanced template.

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> On	 Exchange email	All Choose distribution group	None Exclude distribution group
<input checked="" type="checkbox"/> On	 SharePoint sites	All Choose sites	None Exclude sites
<input checked="" type="checkbox"/> On	 OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group
<input checked="" type="checkbox"/> On	 Teams chat and channel messages	All Choose account or distribution group	None Exclude account or distribution group
<input checked="" type="checkbox"/> On	 Devices	All Choose user or group	None Exclude user or group
<input checked="" type="checkbox"/> On	 Microsoft Defender for Cloud Apps	All Choose instance	None Exclude instance
<input checked="" type="checkbox"/> On	 On-premises repositories	All Choose repositories	None Exclude repositories
<input type="checkbox"/> Off	 Power BI (preview)		

Define policy settings

DLP policy rules include:

Conditions

Determine what types of information you are looking for, and when to take an action.

Exceptions

Prevents the application of a rule for content matching the exceptions.

Actions

When content matches a condition in a rule, you can apply actions to automatically protect the content.

User notifications

Use notifications to educate your users about DLP policies and help them remain compliant without blocking their work.

User overrides

Allows the user to override the policy and share the content.

Incident reports

With a matched rule, you can send an incident report to your compliance officer with details of the event.

Test or turn on your DLP policy

- Use test mode to gauge impact before policy activation.
- Policy matches will be reported to you in emails or through DLP reports.
- Test mode allows you to activate policy tips without enforcing protective actions.
- Policy tips allow users to flag false positives.
- Configure exceptions to the policy to reduce false positives.

Prepare for Endpoint DLP

- Endpoint DLP extends the activity monitoring and protection capabilities of DLP to sensitive items on Windows 10, Windows 11, and macOS
- File type limitations exists
 - Unsupported file types can create opportunities for data loss
- Management of Endpoint DLP policies can be completed by a Compliance Admin
- Devices are monitored by Microsoft Defender for Endpoint
- Devices onboarded for Defender are automatically also onboarded for Endpoint DLP

Prepare for Endpoint DLP (continued)

Endpoint DLP only protects data:

- All Endpoint DLP policies end at the border of the device

Policies allow you to audit or restrict:

- Uploading to restricted cloud service domains
- Access by unallowed browsers
- Copying to the clipboard from protected items
- Copying protected items to USB removable media
- Copying to network shares
- Printing protected items
- Access by unallowed (bluetooth) apps
- Copy or move using RDP

Data loss prevention > Create policy

- Choose the information to protect
- Name your policy
- Locations to apply the policy
- Policy settings**
- Info to protect
- Protection actions
- Customize access and override settings
- Test or turn on the policy
- Review your settings

Service domain and browser activities

Detects when protected files are blocked or allowed to be uploaded to cloud service domains based on the 'Allow/Block cloud service domains' list in endpoint DLP settings.

☒ Upload to a restricted cloud service domain or access from an unallowed browsers ⓘ Audit only ▾

File activities for all apps

Decide whether to apply restrictions for file related activity. Unless you choose different restrictions for restricted apps or app groups below, any restrictions you choose here will be enforced for all apps.

☐ Don't restrict file activity

☒ Apply restrictions to specific activity

When the activities below are detected on devices for supported files containing sensitive info that matches this policy's conditions, you can choose to audit the activity, block it entirely, or block it but allow users to override the restriction

<input checked="" type="checkbox"/> Copy to clipboard ⓘ	Audit only ▾
<input checked="" type="checkbox"/> Copy to a USB removable media ⓘ	Audit only ▾
<input checked="" type="checkbox"/> Copy to a network share ⓘ	Audit only ▾
<input checked="" type="checkbox"/> Print ⓘ	Audit only ▾
<input checked="" type="checkbox"/> Copy or move using unallowed Bluetooth app ⓘ	Audit only ▾
<input checked="" type="checkbox"/> Copy or move using RDP ⓘ	Audit only ▾

Configure global Endpoint DLP settings

Endpoint DLP settings create a framework in which Endpoint DLP policies work

File path exclusions:

- Are applied to all Endpoint DLP policies
- Allow you to limit where your policies are in effect

Restricted apps:

- Are applied when a policy blocks unallowed apps
- Allow you to limit where you can work with protected files

Browser and domain restrictions:

- Are applied when a policy blocks unallowed browsers
- Allow you to limit where you can share protected files

Advanced classification scanning and protection:

- Can use EDM and named entities in your DLP policies

Business justification in policy tips:

- Show default options and custom text box
- Only show default options and/or custom text box

Manage DLP policy alerts

DLP Reports

Provides an overview of DLP violations

Contains DLP policy matches, DLP incidents, and DLP false positives and user overrides reports

Used to fine tune your policies and identify problematic configurations or business processes

Can take up to 24h to update

DLP Alerts Dashboard

Provides a deeper insight into DLP violations

Displays individual alerts

Can aggregate alerts to spot patterns more easily

Defender for Cloud Apps Dashboard

Displays alerts of Defender for Cloud Apps file policies

Shows alerts of all your Defender for Cloud Apps DLP policies

Drill down to specific policies and review only a single policy's matches

Provides a match history and quarantine views

DEMO

Data Lifecycle Management overview

The principles of retention

Retention wins over deletion



Longest retention period wins

Explicit inclusion wins over
implicit inclusion

Shortest deletion period wins

Explain Retention Tools in Microsoft 365

Different tools to retain data:

- Retention Labels
- Label Policies / Retention Label Policies
- Auto-apply Retention labels
- Retention Policies
- Record Management
- Retention Tags and Retention Policies
- In-place eDiscovery & hold
- eDiscovery

To understand the right tools, know:

- Where is the data stored today and in the future?
- Which tools are used in the Microsoft 365 environment?
- Which Retention requirements exist?
- Which requirements does the Adoption Team have?
- Are there other Systems like a DSM on SharePoint to retain and fulfill all requirements?
- Which requirements do you want to fulfill in Microsoft 365

Configure retention policies

Differences between retention policies and retention labels

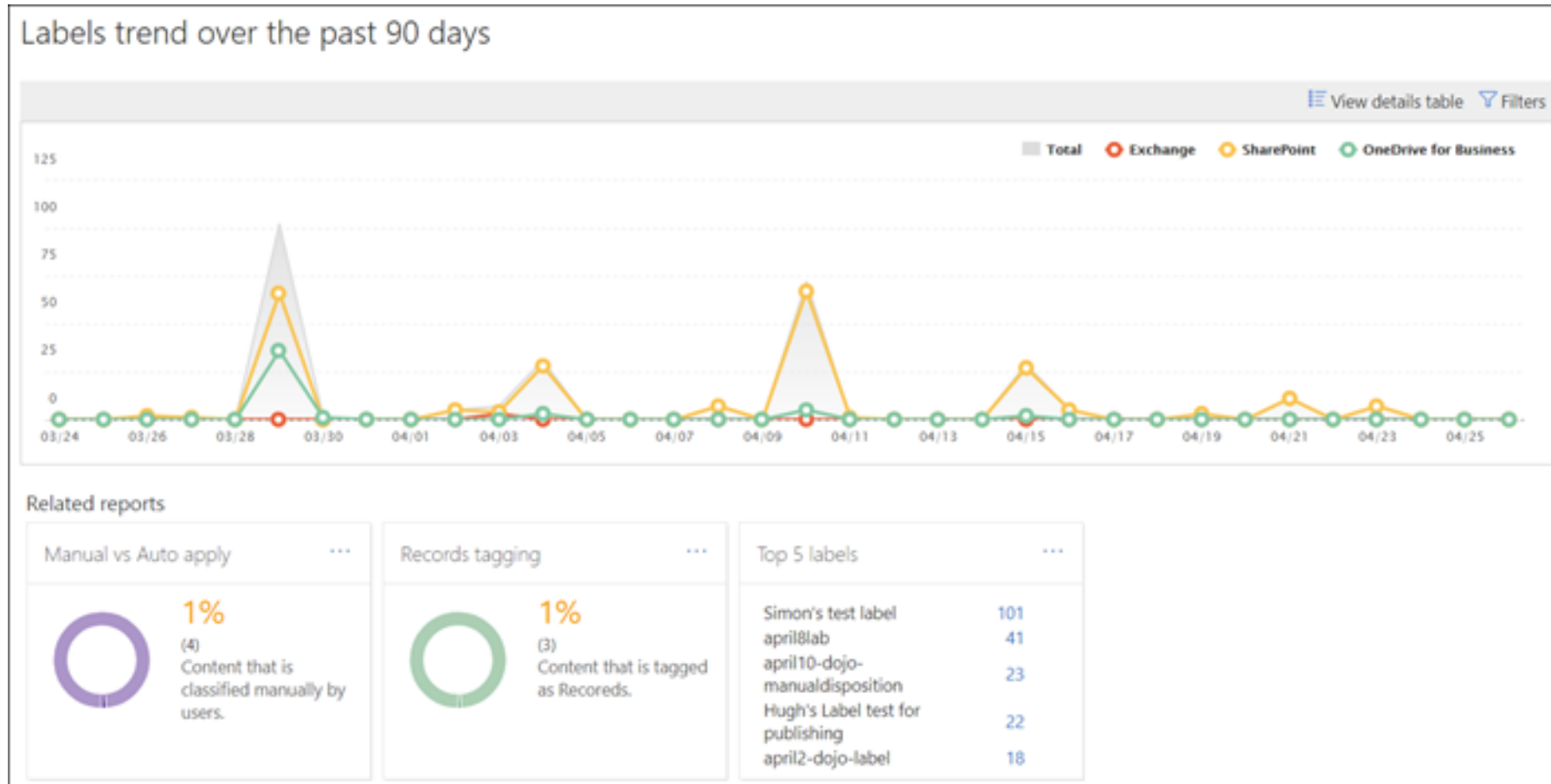
- Retention Policies are focused on service locations.
- Retention Labels are focused on individual items.
 - Retention labels are created for certain kinds of business data.
 - Label policies are used to publish retention labels.

Type	Based on	Travel with the document	Data lifecycle	examples
Retention Policy	Location, product	no	yes	Teams Chat, Junk Folder, SharePoint Site
Retention Label	Single file or email, library, or list	yes	yes, better	Email, document in a library

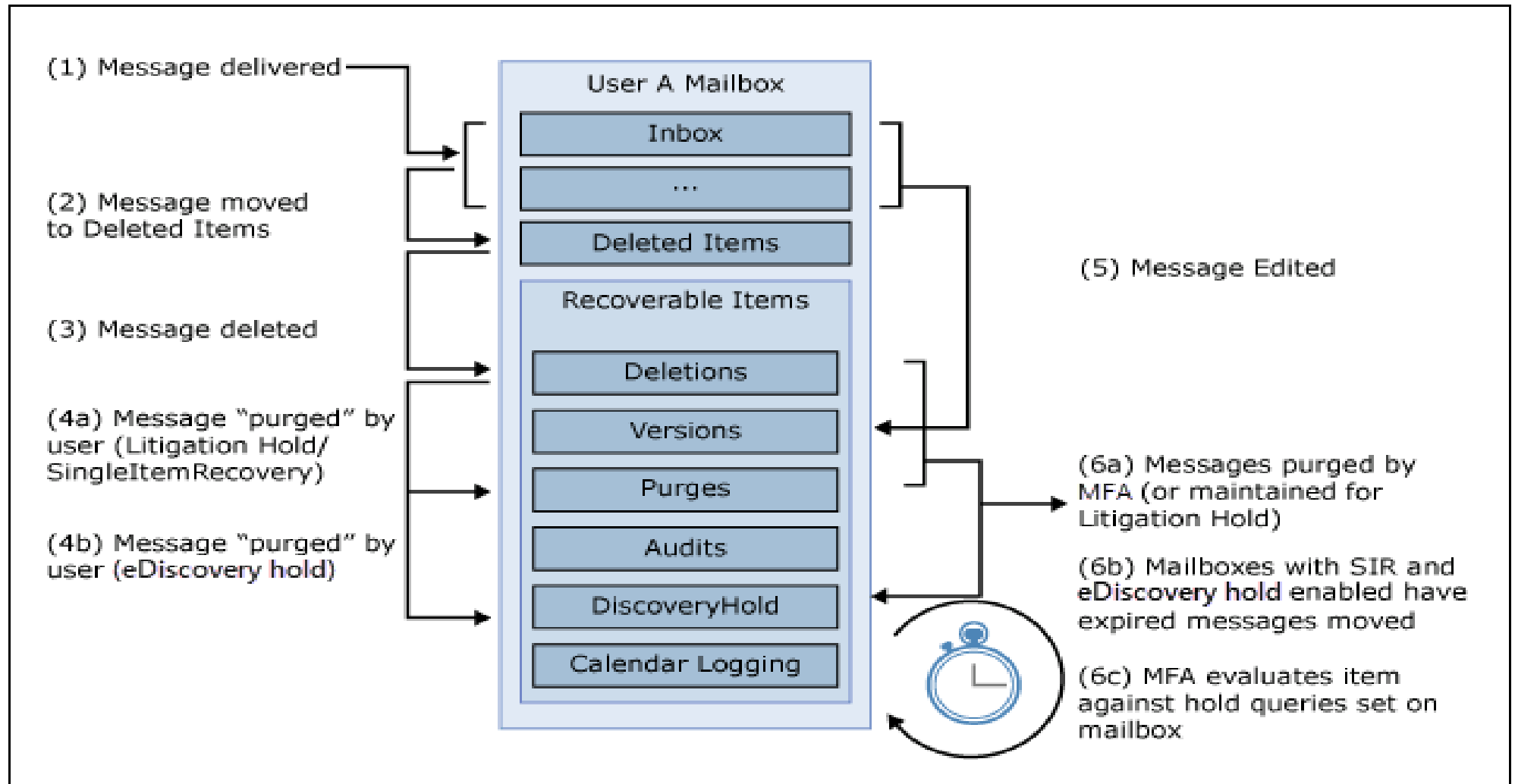
Manage and remediate Data Lifecycle Management

Data Lifecycle Management cards on the Data classification page:

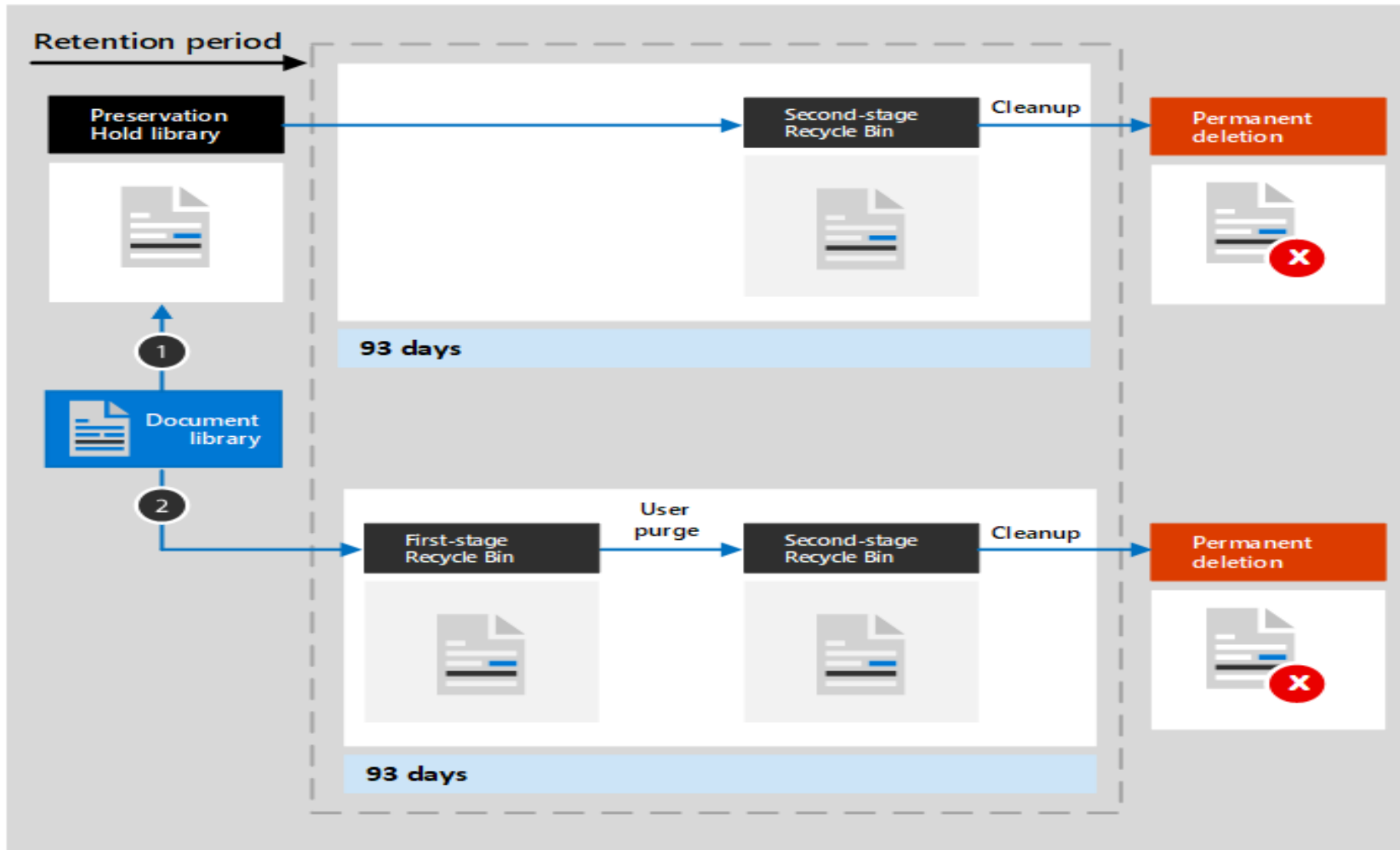
- Top sensitive info types
- Top retention labels applied to content
- Locations where retention labels are applied



Explain retention in Exchange Online



Explain retention in SharePoint Online and OneDrive



Configure file policies in Microsoft Defender for Cloud Apps



File policies can use the Defender for Cloud Apps DLP engine or the same Data Classification Services as DLP policies



You can configure real-time alerts or review alerts via reports



File policies are configured in the Microsoft Defender for Cloud Apps portal



There is no test mode for file policies, actions will be applied as soon as the policy exists



Use the preview functions to see the files your policy would match if you saved it



Policy templates



Filters:

☒ Advanced filters

Type: **File policy** ▾

Severity:

Name:

Category: **Select risk category** ▾

1 - 8 of 8 Templates Hide filters Table settings ▾

Template	Severity ▾	Linked policies	Published	
File shared with unauthorized domain Alert when a file is shared with an unauthorized domain (such as your competitor).	High	0	Mar 19, 2023, 6:17 PM	+
Externally shared source code Alert when a file containing source code is shared outside your organization.	Medium	0	Mar 19, 2023, 6:17 PM	+
File containing PII detected in the cloud (built-in DLP engine) Alert when a file containing personally identifiable information (PII) is detected by our bu...	Medium	0	Mar 19, 2023, 6:17 PM	+
File containing PHI detected in the cloud (built-in DLP engine) Alert when a file containing protected health information (PHI) is detected by our built-i...	Medium	0	Mar 19, 2023, 6:17 PM	+
File containing PCI detected in the cloud (built-in DLP engine) Alert when a file containing payment card information (PCI) is detected by our built-in d...	Medium	0	Mar 19, 2023, 6:17 PM	+
File shared with personal email addresses Alert when a file is shared with a user's personal email address.	Low	0	Mar 19, 2023, 6:17 PM	+

eDiscovery in Microsoft Purview

- Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases.
- eDiscovery tools: Content search, eDiscovery (Standard), eDiscovery (Premium)

Content search	eDiscovery (Standard)	eDiscovery (Premium)
<ul style="list-style-type: none">▪ Search for content▪ Keyword queries and search conditions▪ Export search results▪ Role-based permissions 	<ul style="list-style-type: none">▪ Search and export▪ Case management▪ Legal hold 	<ul style="list-style-type: none">▪ Custodian management▪ Legal hold notifications▪ Advanced indexing▪ Review set filtering▪ Tagging▪ Analytics▪ Predictive coding models▪ And more... 

Auditing in Microsoft Purview

- Microsoft Purview auditing solutions help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations.
- Microsoft Purview provides two auditing solutions: Audit (Standard) and Audit (Premium).

Audit (Standard)



Log and search for audited activities:

- Enabled by default
- Thousands of audited events
- 90-day audit record retention
- Accessed by GUI, cmdlet, and API

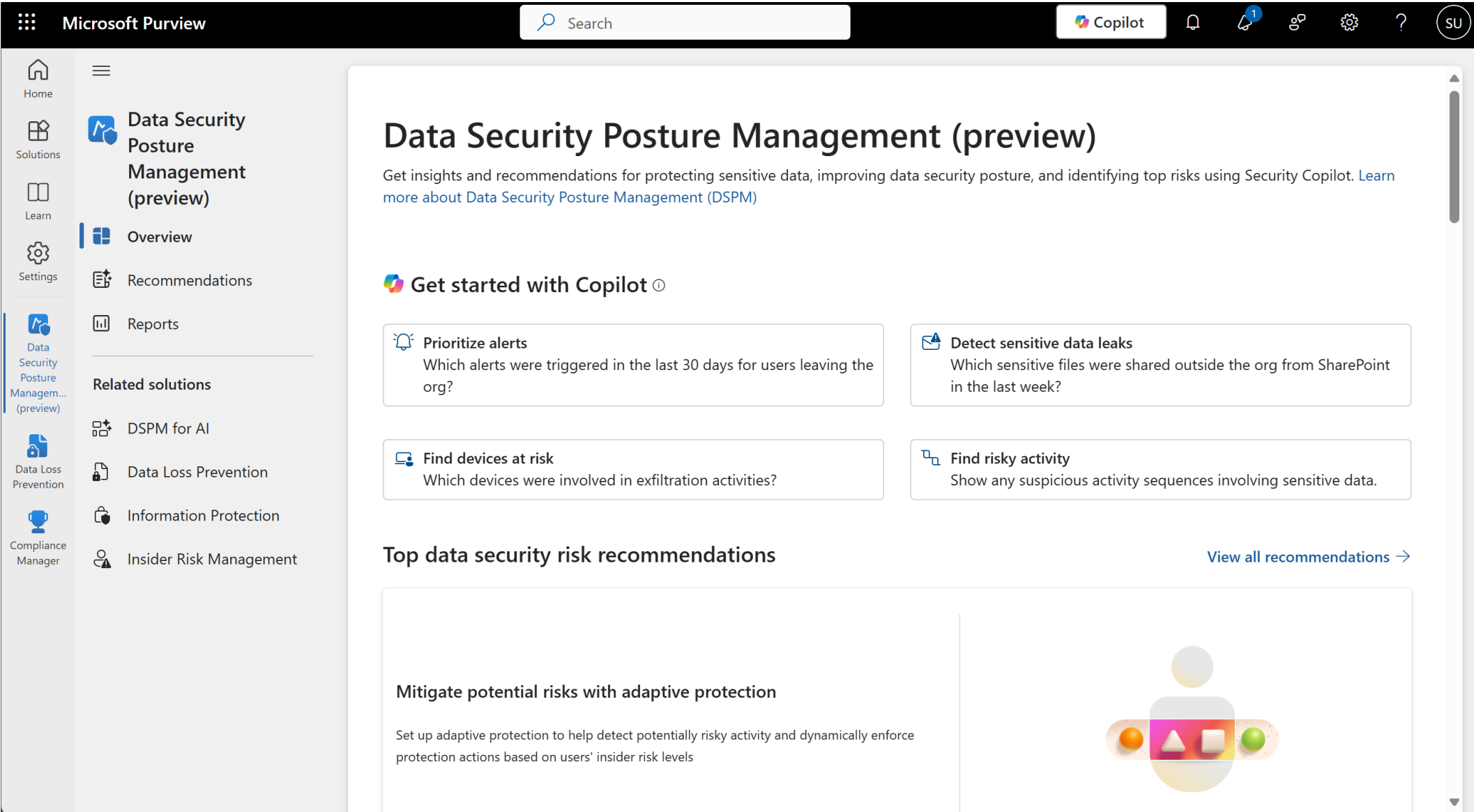
Audit (Premium)



Advanced Audit capabilities:

- Longer retention of audit records
- Custom audit retention policies
- High-value, crucial events
- Higher bandwidth access to API

Data Security Posture Management in Microsoft Purview



Data Security Posture Management for AI in Microsoft Purview

DSPM for AI

Overview

Recommendations

Reports

Policies

Activity explorer

Data assessments

Preview

Data Security Posture Management for AI

Discover and secure all AI activity in Microsoft Copilot and other AI apps. Keep your data safe and stay on track with industry regulations. [Learn more about DSPM for AI](#)

Get started

<input checked="" type="checkbox"/>	Activate Microsoft Purview Audit Get insights into user interactions with Microsoft Copilot experiences.	Required	🕒 7 Minutes
<input type="checkbox"/>	Install Microsoft Purview browser extension Detect risky user activity and get insights into user interactions with other AI apps.	Required	🕒 1 Hour
<input type="checkbox"/>	Onboard devices to Microsoft Purview Protect sensitive data from leaking to other AI apps.	Required	🕒 1 Hour
<input type="checkbox"/>	Extend your insights for data discovery Discover sensitive data in user interactions with other AI apps.	Required	🕒 10 Minutes

Recommendations

Data security

DEMO

CIAOPS Resources



- Blog – <http://blog.ciaops.com>
- Free Office 365, Azure video tutorials – <http://www.youtube.com/directorciaops>
- Free documents, presentations, eBooks – <http://slideshare.net/directorcia>
- Office 365, Azure, Cloud podcast – <http://ciaops.podbean.com>
- Office 365, Azure online training courses – <http://www.ciaopsacademy.com>
- Office 365 and Azure community – <http://www.ciaopspatron.com>
- CIAOPS Github – <https://github.com/directorcia>

[Twitter](#)
[@directorcia](#)

[Facebook](#)
<https://www.facebook.com/ciaops>

[Email](#)
director@ciaops.com

[Skype for Business](#)
[admin@ciaops365.com](skype:admin@ciaops365.com)



Get access to the latest
information by becoming a
Patron

<http://www.ciaopspatron.com>



Questions

That's all folks!

Thanks for attending