## DSMP for AI

| **What to say** | **What to show** |
| --- | --- |
| Navigate to **DSPM for AI** in the Purview console.  Review the **Overview** page and note the policies listed |  |
| Navigate to **Recommendations** and review the additional options including *Secure interactions from enterprise AI apps as shown*. |  |
| Navigate to **Reports** and review the available reports. Filter on the three categories available:   1. Copilot experiences & agents 2. Enterprise AI apps 3. Other AI apps |  |
| Navigate to **Apps and Agents** and review both Apps and Agents. |  |
| Navigate to **Activity explorer**.   * Adjust the timestamp filter as per screenshot. * Explore available filters including:   + **AI App Category** to filter between the 3 catagories.   + Activity type to filter **on AI Interaction**, **Sensitive info types**, **DLP rule match** and **AI website visit**.   + d |  |
| Navigate to **Data risk assessments**   * Review the list of Data Risk Assessments available. * View details of the Default assessment * Review the /teams/datasecuritysampledata/ sharepoint site. |  |
| **References:**   * [Microsoft Purview – Microsoft Adoption](https://adoption.microsoft.com/en-gb/microsoft-security/purview/) * [Notes from engineering - Purview deployment models | Microsoft Learn](https://learn.microsoft.com/en-us/purview/deploymentmodels/depmod-overview) * [What's new in Microsoft Purview | Microsoft Learn](https://learn.microsoft.com/th-th/purview/whats-new?view=o365-worldwide) | The image shows the deployment model to secure and govern Microsoft 365 Copilot agents with Microsoft Purview in four phases, the first phase is to discover the risks and identify gaps, the second is to protect the grounding data, the third is to protect the interactions, and finally the fourth phase is to govern the interactions.Prevent data leak to shadow AI with Microsoft. |