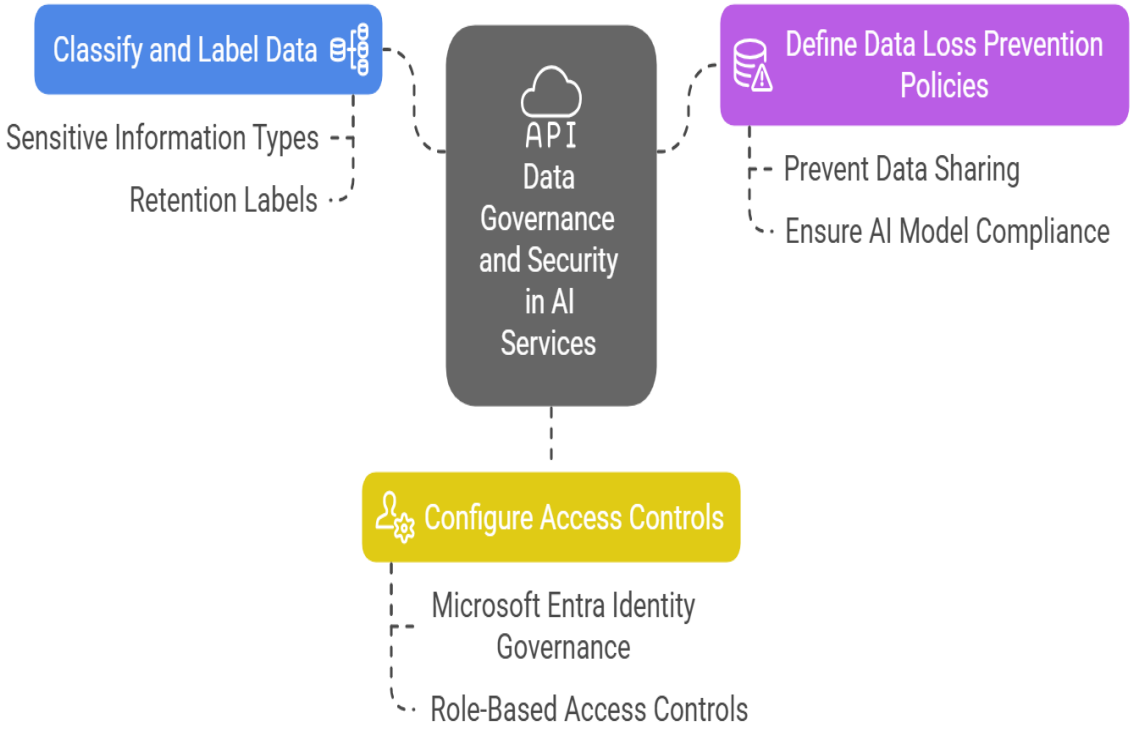
Protecting Content in an environment that uses AI services

To implement controls in Microsoft Purview to protect content in an environment that uses AI services, follow these steps:

1. **Classify and Label Data:**
   - **Sensitive Information Types (SITs):** Use Microsoft Purview to classify data by applying predefined or custom sensitive information types (SITs) that align with the types of content processed by AI services.
   - **Retention Labels:** Apply retention labels to data to control how long content is retained and when it should be deleted, ensuring AI-generated data complies with organizational retention policies.
2. **Define Data Loss Prevention (DLP) Policies:**
   - Set up DLP policies to prevent the accidental sharing or exposure of sensitive data in AI services. These policies can detect and prevent sensitive data from being shared or moved outside the organization or exposed to unauthorized users.
   - Ensure AI models don't access or share data in violation of DLP policies by configuring sensitive actions such as blocking, encrypting, or notifying when violations are detected.
3. **Configure Access Controls:**
   - Use **Microsoft Entra Identity Governance** to manage permissions, ensuring only authorized users and AI services can access sensitive data.
   - Set up role-based access controls (RBAC) to restrict access to classified or sensitive data in Purview.



4. **Monitor and Audit Content:**
   - Enable **audit logging** in Microsoft Purview to track user and AI service activities related to sensitive data. This can help monitor the AI system's interaction with protected content.
   - Use **Data Activity Monitoring** to assess how AI models or services access or use sensitive data, helping to identify any unauthorized access.
5. **Apply Endpoint Protection:**
   - Utilize **Microsoft Defender for Endpoint** to apply security policies and ensure AI services running on devices are compliant with your organization's security posture.
   - Monitor and enforce security measures such as encryption and security baselines on devices that interact with AI-powered content.
6. **Integrate with AI Models:**
   - Integrate Purview's information protection and DLP controls into the workflow of AI services by configuring AI platforms (e.g., Azure AI services) to respect the protection and compliance settings applied in Purview.

Monitor and Audit Content

Tracks user and AI activities to ensure data security

Apply Endpoint Protection

Enforces security policies on devices interacting with AI

Integrate with AI Models

Aligns AI services with data protection settings