Power BI provides various options for managing user access to ensure that data is shared securely and appropriately. Here are the main options:

**1. Roles and Row-Level Security (RLS)**

**Roles:** In Power BI, you can define roles with specific permissions and assign users to these roles. Roles can be created within Power BI Desktop using DAX (Data Analysis Expressions) filters to restrict data access.

**Row-Level Security (RLS):** RLS allows you to restrict data access for given users at the row level. For example, sales managers may only see data related to their regions. You can configure RLS in Power BI Desktop and then publish the model to Power BI Service.

**2. Workspaces**

Workspaces in Power BI are collaboration spaces where you can share content with specific groups of users. There are different types of workspaces:

* **My Workspace:** Personal workspace for individual users.
* **App Workspaces:** Collaborative workspaces that can be shared with multiple users. You can assign roles within the workspace (Admin, Member, Contributor, Viewer) to control access levels.

**3. Apps**

You can create Power BI apps to bundle related dashboards and reports and then share the app with users or groups. Apps provide a controlled way to distribute content to a broader audience while managing access through app permissions.

**4. Permissions and Sharing**

**Dashboard and Report Sharing:** You can share individual dashboards and reports with specific users or groups. When sharing, you can control whether users can share further, build new content with the shared dataset, or just view the content.

**Content Packs:** Although somewhat deprecated in favor of apps, content packs can be used to share datasets, reports, and dashboards with users.

**5. Dataflows and Datasets**

**Dataflows:** Dataflows are used to create reusable data transformation logic that can be shared across different datasets and reports. You can control access to dataflows to ensure that only authorized users can use or modify them.

**Datasets:** You can share datasets across different reports and users. Permissions on datasets can be managed to ensure users have appropriate access.

**6. User Licenses**

**Free License:** Allows users to create and view content in their personal workspace but requires a Pro license to share or collaborate with others.

**Pro License:** Required for sharing content, collaborating with others, and accessing content shared by other Pro users.

**Premium Per User (PPU):** Provides advanced capabilities like AI, paginated reports, and larger dataset sizes, along with sharing and collaboration features.

**Premium Capacity:** Provides organizational capacity for large-scale deployment with advanced features, including larger storage and more computational power. Users accessing content in a Premium capacity only need a Free license if the content is shared within the organization.

**7. External Sharing**

You can share Power BI content with external users (users outside your organization) by adding them as guest users in Azure Active Directory (AAD). External users must have a Power BI Pro license to view shared content unless it's hosted in a Premium capacity.

**8. Azure Active Directory (AAD) Integration**

Power BI integrates with AAD for user authentication and authorization. You can use AAD groups to manage access to Power BI workspaces, apps, and shared content, simplifying user management.

**9. Data Protection and Sensitivity Labels**

Power BI allows you to apply Microsoft Information Protection (MIP) sensitivity labels to datasets, reports, and dashboards to classify and protect sensitive information. These labels help ensure data is handled appropriately according to your organization's policies.

**Conclusion**

Power BI offers a robust set of options for managing user access, from workspace-level permissions to fine-grained row-level security. These options ensure that data is shared securely and appropriately, aligning with organizational needs and compliance requirements.