Copilot for Microsoft 365 Implementation and Adoption

dedalus
mais que cloud computing

Copilot for Microsoft 365

Copilot for Microsoft 365

Implementation and Adoption

The methodology includes the following phases:

- Assessment: Assessment process in collaboration with your organization to understand specific needs and determine how Copilot can best be used. This may involve identifying specific tasks or processes that can be automated or simplified using Copilot, as well as determining which users or teams will benefit most from using the tool.
- Implementation: Following required security measures covering data security, governance, risk, compliance, and Microsoft 365 data lifecycle management.
- Adoption: Conducting workshops that aim to present the product's main features and use cases. We also support the implementation of working groups to exchange experiences and monitor product adoption.
- Support: We ensure ongoing support to help users resolve any issues that may arise such as user and policy management, content management for dataset changes, prompt support, and more.

Copilot Preparation for Microsoft 365

- ✓ Apply Zero Trust principles to Microsoft Copilot for Microsoft 365;
- ✓ Confidentiality labels;
- ✓ Review current access, Microsoft Login ID;
- ✓ Data loss prevention;
- ✓ Copilot Semantic Index;
- ✓ Best practices with SharePoint Online.

dedalus
mais que cloud computing

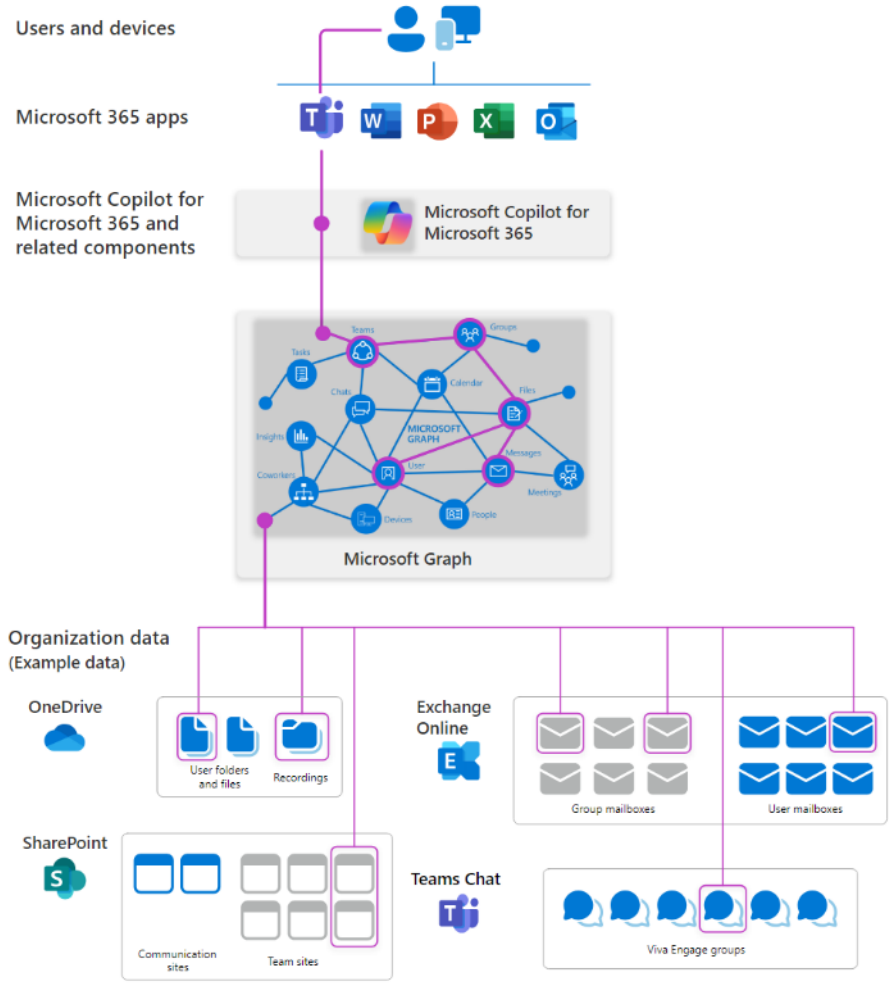
Security for your Tenant

1. Implement or validate your data protection: Prevent your organization's data from being at risk of overexposure or oversharing.

2. Implement or validate your identity and access policies: Prevent bad actors from using Copilot to discover and access sensitive data faster, the first step is to prevent them from gaining access.

3. Deploy or validate your App Protection policies: Use Intune app protection policies, rules that ensure an organization's data remains secure or contained within a managed app.

4. Deploy or validate device management and protection: Detect the activities of bad actors and prevent them from gaining access to Copilot, the next step is to leverage Microsoft 365 threat protection services.



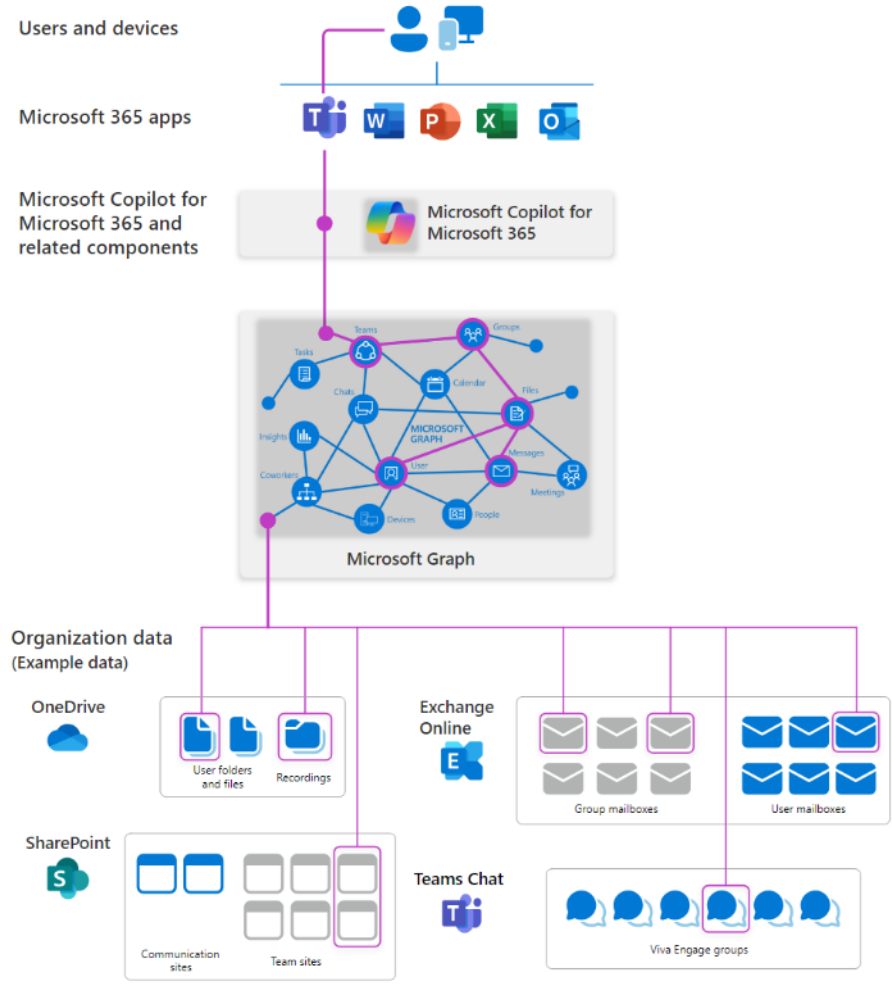
dedalus
mais que cloud computing

Security for your Tenant

5. Deploy or validate your threat protection services: Protect your teams at three different levels – baseline, confidential, and highly sensitive. Introducing Copilot is a good time to review your environment and ensure that appropriate protection is configured (Defend).

6. Deploy or validate secure collaboration for Microsoft Teams: Microsoft provides guidance for securing your teams at three different levels – baseline, confidential, and highly sensitive.

7. Implement or validate minimum user permissions for data: Prevent your organization's data from being at risk of overexposure or oversharing, the next step is to ensure that all users have sufficient access (JEA) to perform their jobs and nothing more.



dedalus
mais que cloud computing