



Microsoft 365
Copilot

XTIUM

Microsoft 365 copilot architecture and **how it works**



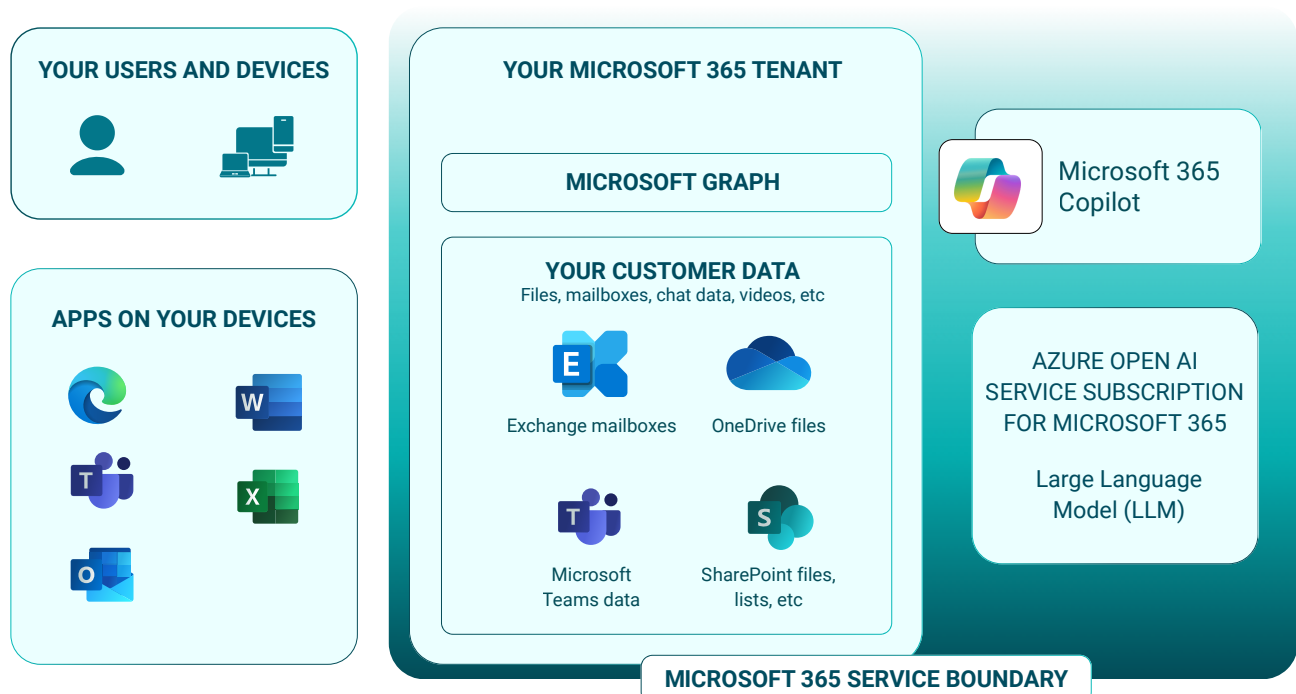
Microsoft 365 Copilot

When you create a Microsoft 365 subscription, you automatically create a tenant for your organization. Your tenant sits inside the Microsoft 365 service boundary, where Microsoft 365 Copilot can access your organization's data.

Operating inside the Microsoft 365 service boundary doesn't grant Copilot tenant-wide visibility. Data access is always scoped to the signed-in user's permissions.

This data includes information that the user can access, including their activities, and the content they create and interact with in Microsoft 365 apps.

Microsoft 365 copilot architecture and how it works



Copilot is a shared service, just like many other services in Microsoft 365. When you use Copilot in your tenant:

- Your customer data stays within the Microsoft 365 service boundary.
- Existing security, compliance, and privacy policies already deployed by your organization secure your data.

This article describes **how Microsoft 365 Copilot works, including the data flow in a user prompt, how Copilot accesses data, and how Copilot honors Conditional Access and multifactor authentication (MFA).**

Intended for **IT admins, security teams, and technical decision-makers** who want to understand the core architecture of Microsoft 365 Copilot. It focuses on data flow, permissions, and security boundaries.

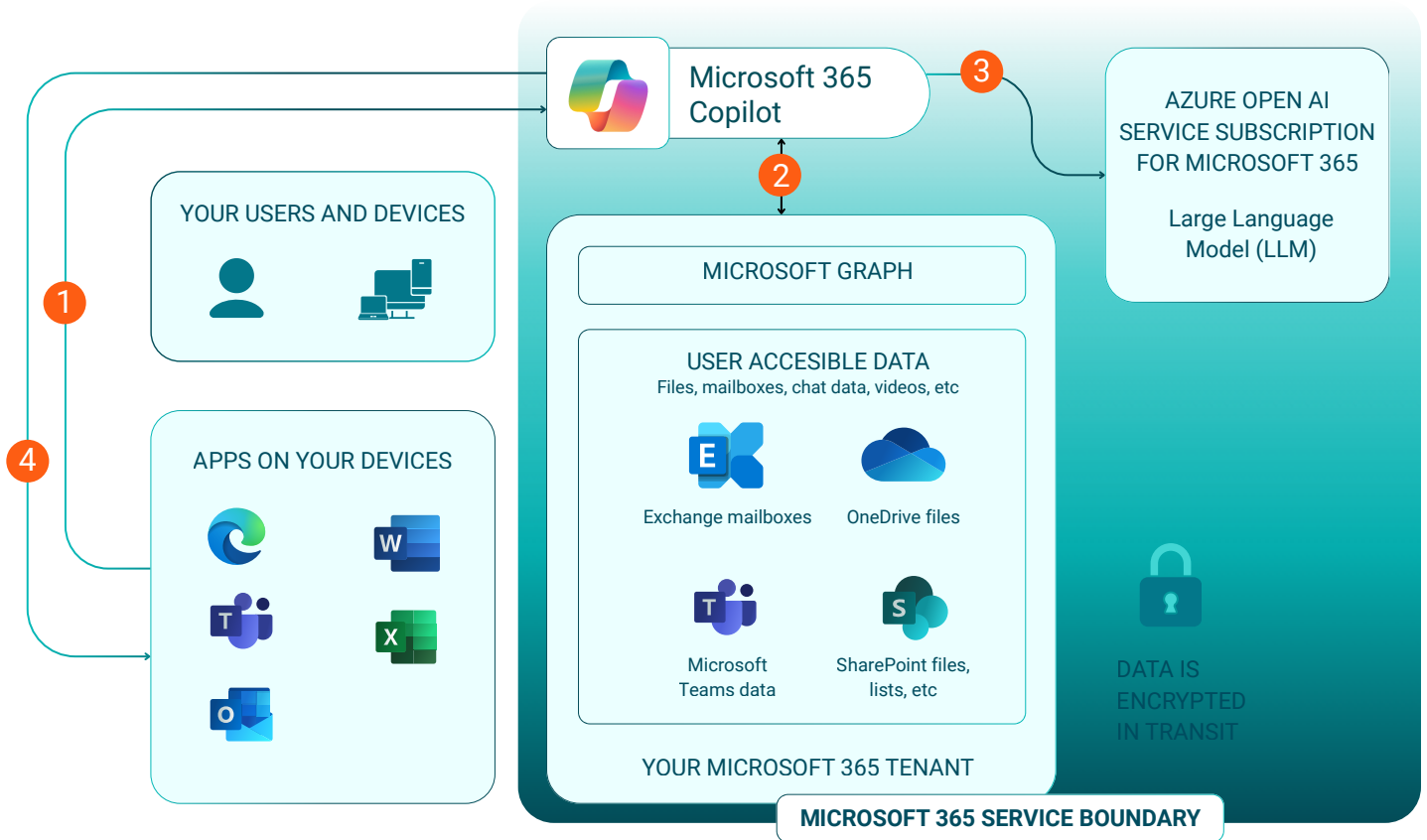
This article applies to:



User prompts and Copilot responses

When users open a Microsoft 365 app, like Word or PowerPoint, they can use Copilot to get real time data.

The following diagram provides a visual representation of how a Copilot prompt works.



Let's take a look

1

In a Microsoft 365 app, a user enters a prompt in Copilot.



2

Copilot preprocesses the input prompt by using **grounding** and accesses Microsoft Graph in the user's tenant.

- Grounding improves the specificity of your prompt, and helps you get answers that are relevant and actionable to your specific task. The prompt can include text from input files or other content Copilot discovers.
- The data Copilot uses to generate responses is encrypted in transit.

3

Copilot sends the grounded prompt to the LLM. The LLM uses the prompt to generate a response that is contextually relevant to the user's task.



4

Copilot returns the response to the app and the user.

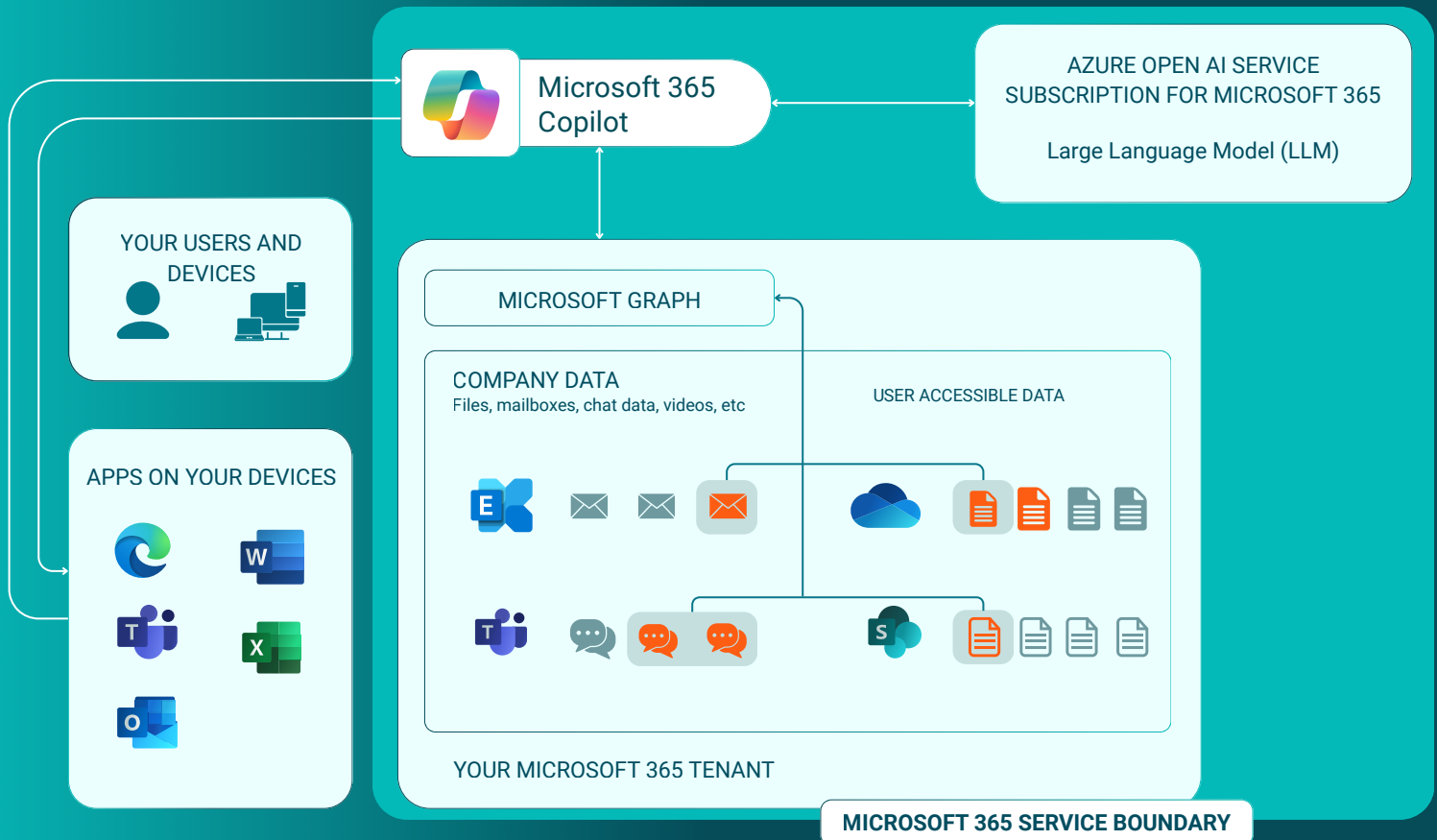
User access and data privacy

Copilot only accesses data that an individual user is authorized to access, based on, for example, existing Microsoft 365 role-based access controls.

Copilot doesn't access data that the user doesn't have permission to access.



The following diagram provides a visual representation of how Copilot and user access work together.



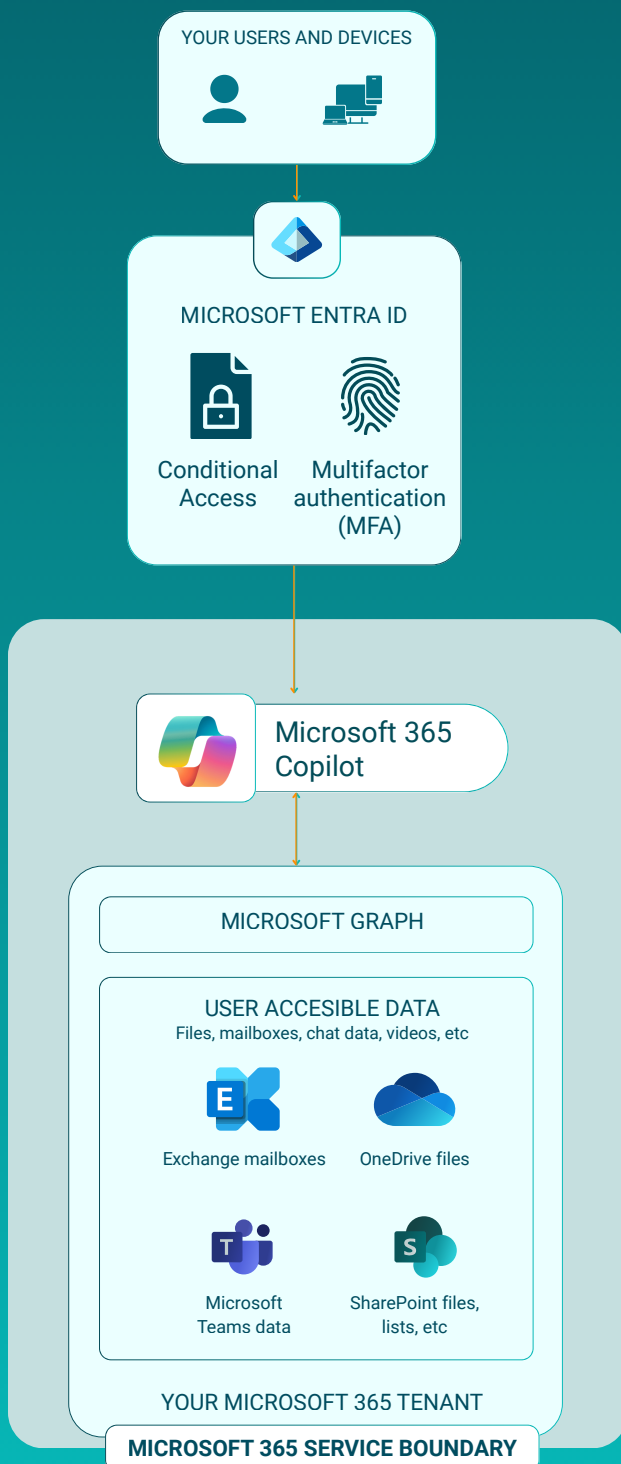
Let's take a look

- On devices, users open an app and enter a prompt in Copilot.
- Copilot uses Microsoft Graph to access user data that's in the user's unique context. This user data includes emails, chats, and documents that the user has permission to access. Microsoft 365 services help control access and security to your organization's data. These services include Restricted SharePoint Search (RSS), SharePoint Advanced Management (SAM), and Microsoft Purview. To learn more, see [Microsoft 365 E3 and E5 feature comparison list for Microsoft 365 Copilot](#).
- Copilot can't access data that the user doesn't have permission to access. In the diagram, the grayed-out data represents data that Copilot can't access.
- When a user enters a prompt and Copilot responds, the interaction is stored in the user's Copilot chat history. Users can review and reuse their previous prompts. They can also delete their chat history .



Copilot honors Conditional Access and MFA

Copilot honors Conditional Access policies and multifactor authentication (MFA).



This means

If you enable and configure Conditional Access policies, make sure your users can access Microsoft 365 services. **You can manage access based on conditions you configure**, including enforcing device compliance policies you set.

Copilot uses the same MFA features you configure for your tenant. **With MFA, like all Microsoft 365 services, users must provide multiple forms of verification** before they're allowed to access Copilot.

If your tenant uses security defaults, then MFA is enabled by default. If MFA isn't enabled, then Microsoft recommends enabling MFA.

If you use Microsoft Intune, you **can use Intune compliance policies and Conditional Access together**.



Microsoft 365
Copilot

Copilot Is Technology.
Business Value Requires a Partner.

Buying Microsoft Copilot directly gives you access to the technology.

Choosing XTIUM gives you a partner responsible for helping you realize value from that investment.

From readiness and deployment to adoption, governance, support, optimization, and renewal management, XTIUM helps organizations turn Microsoft Copilot into measurable business outcomes, **not just another software license.**



The Four Reasons To Choose XTium

1 We Help You Realize Value — Not Just Activate Licenses

Most organizations don't struggle with buying Copilot.

They struggle with:

- **Adoption**
- **Governance**
- **Change management**
- **Measuring ROI**
- **Scaling AI successfully**

XTium helps organizations move beyond experimentation and create a roadmap that delivers meaningful business outcomes.

Outcomes We Help Drive

- ✓ Increased employee productivity
- ✓ Faster decision making
- ✓ Reduced manual work
- ✓ Better employee experiences
- ✓ Stronger customer engagement
- ✓ More value from your Microsoft investment

2 We Bring 25+ Years of Microsoft Expertise

AI adoption doesn't happen in isolation.

It depends on your Microsoft environment, security posture, data governance, collaboration tools, user experience, and licensing strategy.

As a Microsoft partner for **more than 25 years** and a **Tier 1 Microsoft CSP**, XTium helps customers **maximize the value of Microsoft technologies across the entire organization, not just Copilot.**

Whether you're evaluating licensing, preparing your environment, improving security, or driving adoption, our team understands the complete Microsoft ecosystem.

3 We Support Your Entire Technology Ecosystem

Most providers can help you buy Copilot. Few can help you operationalize it.

Because XTium is a full-stack managed services provider, we can support nearly every aspect of your technology environment, including:

- ✓ Microsoft 365
- ✓ Security & Compliance
- ✓ Managed Network Services
- ✓ Enterprise Service Desk
- ✓ UCaaS & CCaaS
- ✓ Cloud & Infrastructure
- ✓ Endpoint & Desktop Services
- ✓ AI & Automation

THE RESULT

One partner. One strategy. One accountable team.
Not multiple vendors pointing fingers when challenges arise.

4 We're Large Enough to Lead. Small Enough to Care.

Many organizations choose between:

Large Providers
Enterprise expertise. Limited personal attention.

Boutique Providers
Personal relationships. Limited capabilities.

XTium delivers both.

We're recognized among the industry's leading managed services providers while maintaining a customer-first approach built on long-term relationships.

When you call, you're not opening a ticket with an anonymous support queue. You're working with people who know your business, understand your environment, and are invested in your success.

What You Get With XTIUM + Microsoft

CAPABILITY	MICROSOFT DIRECT	TRANSACTIONAL RESELLER	XTIUM + MICROSOFT
Microsoft Copilot Licensing	✓	✓	✓
Licensing Guidance & Optimization	Limited	Limited	✓
AI Readiness Assessment	✗	✗	✓
Security & Governance Planning	✗	✗	✓
Copilot Deployment Services	Limited	Limited	✓
User Adoption & Training	Limited	✗	✓
Ongoing Usage Monitoring	✗	✗	✓
ROI & Value Realization Reviews	✗	✗	✓
Renewal & Cost Optimization	✗	Limited	✓
Microsoft Environment Expertise	Limited	Varies	✓
Security & Compliance Support	✗	Varies	✓
End-to-End Managed Services	✗	✗	✓
Single Point of Accountability	✗	✗	✓

Why Buyers Ultimately Choose XTIUM

They don't need another software vendor.

They need a **partner**.

A partner that understands **Microsoft**.

A partner that understands **AI**.

A partner that understands **security**.

A partner that understands **adoption**.

A partner that understands **business outcomes**.

And a partner that can support their entire technology ecosystem — not just a single license.

That's why organizations choose XTIUM.

XTIUM combines the power of Microsoft Copilot with the strategy, governance, adoption expertise, and managed services needed to turn AI into measurable business outcomes.

