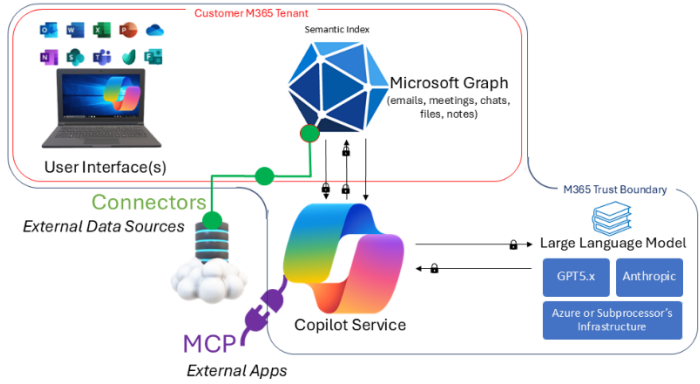
22 Extending Copilot Beyond Microsoft 365

Microsoft 365 Copilot natively connects data in the Office suite to LLMs. But what if users want to connect Copilot to other data sources outside Microsoft 365, such as external databases, document systems, or CRMs?

What if people want to make Copilot do more with the data, such as making charts, summarizing documents, translating languages, or sending emails?

This chapter covers **Connectors and MCP Servers**, which can make Copilot more extensible and better suited for an organization's specific needs. It also mentions Plugins, a slowly fading integration technique.



Connectors interface with external data sources that are indexed by the Microsoft Graph, and **make external content available to Copilot** for search and content generation. **Model Context Protocol (MCP)** connects to apps beyond the Microsoft 365 ecosystem to **add skills and capabilities to Copilot**. **Agents** autonomously perform tasks and makes decisions based on data from the environment. Connectors will be covered first, followed by MCP. For Agents, see Chapter 13.

Augmenting Prompts with Connectors

Microsoft 365 Copilot is natively built to augment your prompts with data from within Microsoft 365. If the valuable data of an organization is stored elsewhere, like in a document management system or customer relationship database, there are choices to interact with it via a large language model.

A) **Use the SaaS / storage provider's generative AI features from within their product**, continuing to use their software interface to interact with the data in their system.

B) **Connect the data source to Microsoft 365 via a Connector to the Graph API**. Connectors allow the user to stay within the Microsoft Copilot experience, and augment their prompt with information from external data sources.

Microsoft 365 Copilot Connectors are a set of APIs and tools that pull data from external sources, transform it into a format that can be indexed and searched, and then push it to the Microsoft Search index.

Think of a Connector like a link from one library's electronic catalog to another, giving your librarian a larger set of books you can access.

What Data Sources Can Connect?

There are over 100 (and counting) Copilot connectors to a variety of Microsoft and third-party data sources. They bring external data into the Microsoft Graph and make it accessible across Microsoft 365's apps **with no custom development required.**

Here are **some of the most recognizable external data sources with pre-built Microsoft Graph connectors:**

1. **Azure Data Lake Storage Gen2** - You can search for files stored in Azure Blob Storage and Azure Data Lake Gen 2 Storage accounts.
2. **On-premises File Share** - Indexes unstructured data in SMB file shares.
3. **Azure File Share** - Indexes unstructured data in this Azure storage system.

4. **Salesforce -** Indexes CRM contacts, opportunities, leads, accounts, and Salesforce Knowledge articles.
5. **ServiceNow –** accesses knowledge base articles, catalog items, incidents, and change requests.
6. **Jira –** Indexes issues and tickets from Jira Cloud or Jira Data Center.
7. **Confluence –** References pages and blogs from Confluence Cloud or on-premises deployments.
8. **GitHub –** Indexes issues, pull requests, and documentation from GitHub Cloud or GitHub Server.
9. **Google Drive –** Accesses files and documents stored in Google Drive!
10. **Amazon S3 –** Indexes objects stored in Amazon S3 buckets.

More updated information about each connector can be found on Microsoft's site.[1] Additional 3rd party sources can connect to the Graph via Microsoft partner APIs.[2]

How Connectors Work

Graph API technology is not new with Copilot. It's been in the SharePoint Enterprise Search toolbox for some time. This integration not only enhances Copilot's data sources but makes the external data to other Microsoft Search tools (like the search bar in SharePoint Online).

The connectors work by adding context and content from the third-party source before a prompt is sent to the language model. Connectors are not scanning data in real-time, so if the source system has data that is frequently changing, there is a delay of minutes or hours before the content might be crawled and is available in Copilot. For example, if your organization uses Jira for project management, a connector could allow Copilot to access Jira data to provide updates on *daily* project status or help with *non-real-time* issue tracking, directly within Microsoft 365.

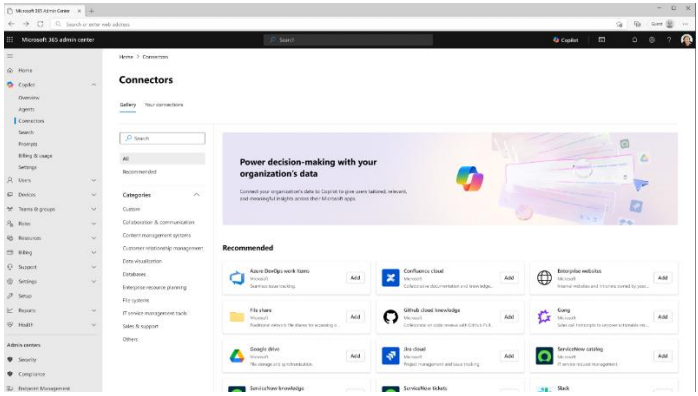
If your organization has Microsoft 365 Copilot licenses, connector grounding in Copilot is included, and **no extra charges apply**. The third-party, however, may charge for their APIs.

Configuring a Connector

Implementing Copilot connectors for Microsoft 365 involves a few key steps to ensure that your line-of-business data is ingested into Microsoft Graph, allowing Copilot to reason over your enterprise content.

The simplest example of a Connector to try is to connect the Microsoft Graph API to search your company's website. Try that with the following steps:

1. Sign into the Microsoft 365 admin center *as an admin*.
2. Navigate to Copilot, then Connectors. You should see a screen like this:



3. After selecting "Enterprise website," you can accept the defaults

or

4. Follow the steps to name the connection, configure the settings, choose the properties that are indexed, manage authentication, register the schema to apply semantic labels and property attributes to the content, set refresh (reindex) times, and rollout.

Creating a Custom Connector

There may be data sources that cannot yet connect to the Copilot API. **The programming needed to do so is not trivial,** but there may be a business case to build your own connector rather than rent one as service. Microsoft provides a Learn module to start configuring a connector where Microsoft nor its partners already have one.[3]

Too Much of a Good Thing?

The number of connectors that can augment a single Copilot prompt at once is not explicitly stated by Microsoft. However, they're not infinitely scalable.

Microsoft 365 Copilot connectors enforce a few key limits to be aware of. Each connection can define up to 128 schema properties, and **each indexed item is capped at 4 MB of parsed text content (roughly 1,400 pages)**. Group administration is throttled at 1,000 requests per second, and a single tenant can have no more than 100,000 external groups. If any threshold is exceeded, Microsoft Graph returns a 429 Too Many Requests error and temporarily blocks further requests. It's safe to say that Copilot can handle a significant volume of data and activity from multiple connectors simultaneously for all but the largest and most active searchers.

There are other constraints to consider. Connectors are indexed daily, and while they extend Copilot's knowledge, they rely on the quality of the external data. **If the data is not well-organized or clean, it may not be as useful for Copilot.** Recall or glance back at Chapter 18 for ways to improve data accuracy.

Protecting Data within Connected Apps

The data coming into Copilot via Microsoft Graph API connectors can be protected from overexposure when an admin:

- Sets Access Control Lists (ACLs) - Choose groups and their permissions for the content in your external data source when indexing connector items. This helps protect sensitive data from unauthorized users.
- Controls Search Permissions - Decide which users in your organization can see each item through the connectors. Some connectors can sync non-Entra ID users and groups, which are synced automatically by the connector and managed via the Microsoft Graph connectors API.
- Adjusts Connection Settings - Regularly check and change the connection settings to make sure that the data exposure matches the organization's policies and compliance requirements. Note that access permissions cannot be updated after a connection is created. If permission settings need to change, the connection must be deleted and recreated.
- Tracks and Audits – Use the compliance monitoring and audit tools from Microsoft Purview to monitor how data is accessed with Microsoft 365 Copilot, including prompts, Copilot responses, and references to connector content from those interactions. For deeper

API-level monitoring, such as tracking which applications are calling Microsoft Graph connector APIs, use Microsoft Graph activity logs routed to an Azure Monitor Log Analytics workspace.

Augmenting Copilot's Skills with Tools

Connectors add more data to Copilot's search sources, **but Tools add more skills** to Copilot. Rather than just using data, Tools allow Copilot to push and pull data from other sources.

Those tools may include connectors, MCP servers, APIs, agent actions, and, in some cases, plugins. The label matters less than the business outcome. The better question is - what does Copilot need to know, access, or do to help the user complete the task?

Unplugging Plugins

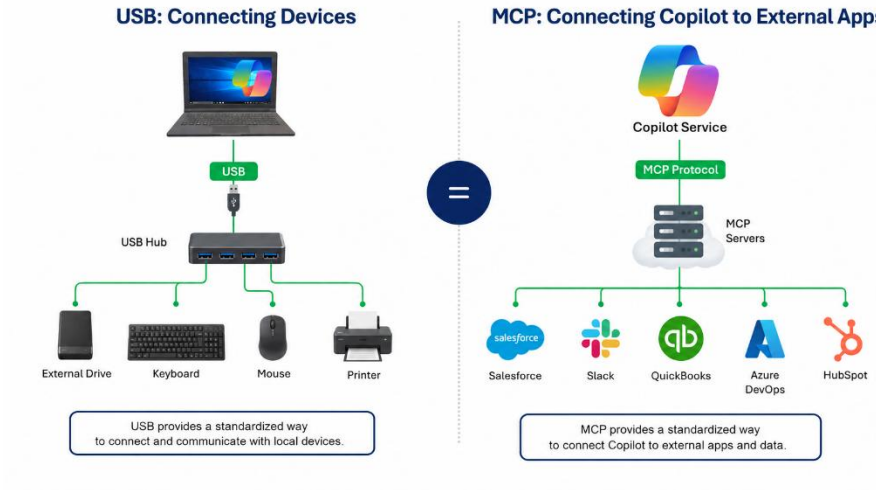
Plugins were an important early way to extend Copilot, and they may still appear in parts of the Microsoft 365 Copilot experience. But they should not be treated as the main forward-looking architecture. Instead, the industry is adopting MCP (Model Context Protocol).

Model Context Protocol is Plugging Away

MCP gives AI systems a more standardized way to discover and use tools exposed by other systems. In practical terms, connectors help Copilot know more, whereas MCP servers help agents do more.

Where a connector might help Copilot find a customer support policy or summarize a set of case notes, an MCP server might let Copilot check live inventory, retrieve current customer details, create a ticket, update a record, or trigger a business workflow.

Just as USB gave hardware a single universal standard to connect any device to any computer, MCP gives AI a single universal standard to connect any data source or tool to any AI system — without custom integrations for each combination.



What MCP Servers can be Plugged in?

Copilot can interact with data from a wide variety of sources via MCP. Copilot can connect to multiple third-party MCP servers at once. For instance, a sales team could have Copilot connected at the same time to Salesforce (for CRM data), HubSpot (for marketing pipeline), ServiceNow (for IT tickets). Copilot could reply to a prompt like "Tell me about customer XYZ" with information from tickets, files, documents, and tasks across multiple work-related third-party SaaS, saving a lot of time and data collating. Microsoft requires that third-party MCP servers undergo a certification process before being made available to all users, and they're governed centrally through the Agent 365 admin center.

MCP Provider	Product	Functionality
Microsoft	Learn Docs MCP Server	Lets an agent answer questions from Microsoft Learn documentation and technical guidance.
Microsoft	Dataverse MCP Server	Provides access to business data and actions in Dataverse-backed applications.
DocuSign	DocuSign MCP	Supports document agreement workflows, such as retrieving envelope status or interacting with signing processes.
Atlassian	Atlassian Rovo MCP Server	Connects agents to Jira, Confluence, Jira Service Management, Bitbucket, and Compass.
Zapier	Zapier MCP	Exposes actions across many SaaS apps so agents can trigger workflows and retrieve live business data.

In the other direction, an organization could deploy the Work IQ MCP server to expose Microsoft 365 tenant content to AI agents through MCP. That enables third-party tools and agents to read, create, update, and delete Microsoft 365 content, invoke Copilot for natural-language reasoning, and discover API schemas, all through a single MCP endpoint. This is the newest capability and isn't well proven yet, but third-party SaaS providers will be experimenting and touting their integrations.

Note external apps are beyond the Microsoft 365 Trust Boundary, and should be treated with API security and Secure Software Development Life Cycle (SSDLC) principles.[4]

One MCP Server Every Organization *Might* Try

One of the MCP servers that Microsoft offers is to Microsoft Learn, their website for support and engineering documents. A user with a **Microsoft 365 Copilot add-on license** accessing the Microsoft Learn MCP server (as a federated connector) from within a Microsoft 365 tenant **does not consume Copilot Credits**. It's a great way to make a Copilot agent that only pulls from the source of truth for content about Microsoft products.

Protect Data Coming in and out of Plugins

When using MCP, it is important to ensure that data is protected as it moves in and out of Copilot. This can be achieved through encryption, access controls, and other security measures. Admins should carefully review the security features of any plugins they use to ensure data is adequately protected. The plugin crosses the Microsoft 365 Trust Boundary, so Agent 365 and its capabilities (Entra ID agent identities, Purview monitoring, and Defender protections) to best secure MCP connections.

Connectors or MCP: Which to Use When?

Connectors and MCP servers solve different problems, and they often work together.

Connectors are used when Copilot needs to understand more. They bring external content into scope so Copilot can search, summarize, and reason over it.

MCP servers are used when Copilot needs to do more. They expose tools that agents can call at runtime — pulling live data, triggering workflows, or updating systems.

For example:

- A connector might make CRM data searchable so Copilot can summarize customer history
- An MCP server might let an agent create a new opportunity, update a record, or trigger a workflow in that same CRM system

Connectors in the Microsoft Graph can be thought of one-way, (outside in). Connectors do not send data back to the external source. MCP can.

Use both when you need Connectors for historical context and MCP servers for live actions.

Copilot Studio

Copilot Studio provides a portal for creating, managing and publishing Copilots to channels like Teams, Copilot Chat, mobile apps, and websites.

It's a web-based development tool that allows people to create, test, and deploy custom Copilots for Microsoft 365. With Copilot Studio, you can:

- Use a drag-and-drop interface to design the user interface of your Copilot, including buttons, menus, cards, and forms.
- Define the logic and behavior of your Copilot using JavaScript or TypeScript, with access to built-in libraries and APIs for Copilot, Teams, and Outlook.
- Integrate a Copilot with external data sources and services using connectors or custom REST calls.
- Preview and debug your Copilot in a live environment, with the ability to edit code and see changes in real time.
- Publish your Copilot to a specific tenant, channel, or user group, or share it with the wider Copilot community.

An organization might use Copilot Studio to build a tailored AI assistant for their website. A custom copilot can assist with product knowledge questions and order management, providing a multi-turn chat interaction with the organization's real-time data. For instance, it can use the company's public website data, including product information, to answer customer queries. For more critical topics like account management, which involve customer details, the custom Copilot can interact with the order management system, following a specific conversational flow designed by the company to match their processes.

If a pro developer has already written a *message extension* for Teams or Outlook, then that is *portable to Copilot as a plugin*. If you're a semi-pro or savvy DIY developer, then the Copilot Studio is a capability to create custom Copilots. Microsoft Foundry is best for enterprise-wide or high-stakes AI systems.

Studio Strategy and Security Considerations

It's a widespread agreement that Large Language Models were just the beginning of a set of relatable AI breakthroughs. Many believe that agents are the next step in the progression towards machines tackling repeatable day-to-day tasks. They're more pliable than robotic process automation and digital twins. The low code nature of Copilot Studio makes it available to citizens and professional developers alike.

Copilot Studio and its agents bring on a similar set of security and governance challenges as Power Platform, which in some cases, has enabled business users to create apps that unknowingly create security holes. The same risk exists in agents, so governance around role-based access control, data encryption, API security, and other aspects should be planned before widespread adoption.

Develop to Differentiate

Mining your most valuable data may be the most valuable investment you can make outside of Copilot. Copilot Connectors (i.e. Graph APIs) are mature ways for organizations to leverage external data via Copilot. Unless your organization's crown jewels are in a proprietary database, try first to use Microsoft or their partners' existing API connectors.

MCP servers connect third-party systems into the LLM and allow two-way interaction. They'll most often be configured by the software manufacturer, but it's possible for an organization to create their own. When doing so, it is important to ensure that they do not impact Copilot's performance or compromise data security.

And for organizations with unique needs, Copilot Studio provides a set of custom tools that can create a unique end-user experience. Developers will make a big difference with Copilot.

---

[1] **https://learn.microsoft.com/en-us/microsoftsearch/connectors-overview**
[2]**https://www.microsoft.com/microsoft-search/connectors/?category&query**
[3] **https://learn.microsoft.com/en-us/graph/connecting-external-content-build-quickstart**
[4] **https://www.paloaltonetworks.com/cyberpedia/what-is-secure-software-development-lifecycle**