

# Techorama

ALL-STAR SPORTS EDITION

Supercharging GitHub Copilot:  
From Custom Instructions to  
Model Context Protocol



# Supercharging GitHub Copilot: From Custom Instructions to Model Context Protocol

Level: Intermediate



**Josh Johanning**

Senior DevOps Architect





# Josh Johanning

Senior DevOps Architect, GitHub  
FastTrack team

- Email: [joshjohanning@github.com](mailto:joshjohanning@github.com)
- Website: [josh-ops.com](http://josh-ops.com)
- From: Madison, WI, USA

Loves:

- DevOps, automation, and security
- Mixing craft cocktails
- Two cats
- Daughter (age 9 months!)

# Resources / Slides

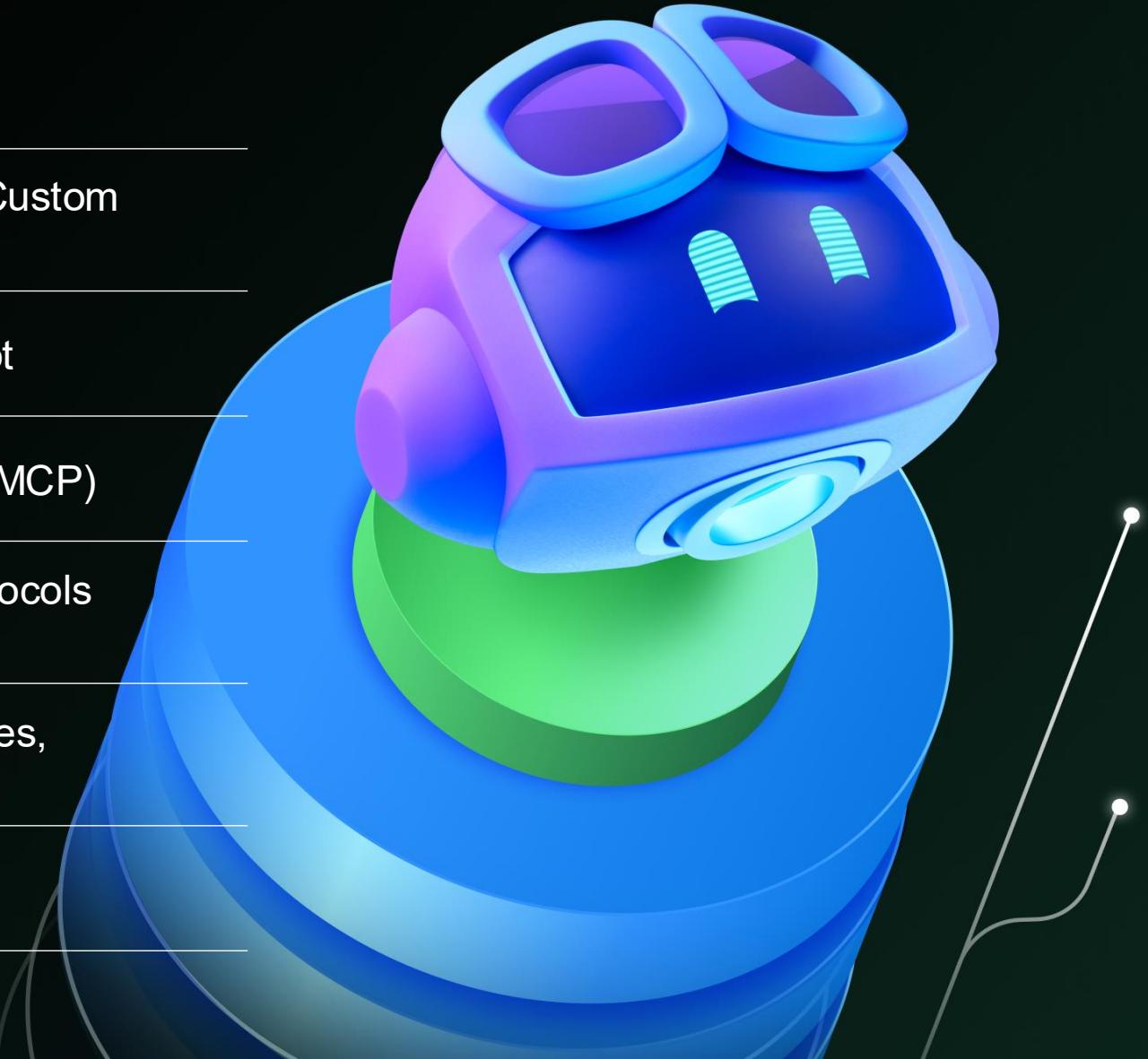
*shared again at the end*

[gh.io/josh-copilot-talk](https://gh.io/josh-copilot-talk)



## Agenda

- 01** Introduction
- 02** Native Copilot Features and Custom Instructions (*and Demo*)
- 03** Understanding Tools in Copilot
- 04** The Model Context Protocol (MCP)
- 05** Building Custom Context Protocols (MCP) (*and Demo*)
- 06** MCP Server Hosting, Registries, and Policies
- 07** Q&A and Survey!



# Part 1: Introduction

Two powerful customization approaches

# Today's Focus

- **How we got here:** Brief histories of Copilot and Copilot extensibility
- **Custom Instructions and native Copilot features**
  - Tell Copilot HOW to write code (your style, your standards)
  - **Start today:** Custom instructions work right now, no setup required
- **Model Context Protocol (MCP):**
  - Give Copilot WHAT it needs to know (your data, your tools)
  - **Scale tomorrow:** MCP for dynamic context and enterprise deployment
    - Or as I'll show you, start today, it's not as scary as it sounds ☺

# The Evolution of GitHub Copilot



From code completion to AI assistant



2021-2022

Launched as autocomplete tool



2023

Chat and command integration



2025

MCP adopted as universal standard; coding agent



2026

??? Stay tuned ☺



2024 into early 2025

Improved workspace context, edit mode, agent mode

# Part 2: Native Copilot Features and Custom Instructions

Native customization options

# Custom Instructions Overview

**Custom Instructions** let you shape Copilot's behavior:

- Native to GitHub Copilot and VS Code
- Simple configuration files
  - Version controlled and shared!
- No servers to deploy, no infrastructure needed

You use custom instructions to tell Copilot HOW to write code for you and your team

Four scopes of configuration today

# Levels of Custom Instructions

1. Personal instructions: Personal preferences
    - Web-only ([github.com/copilot](https://github.com/copilot))
  2. Repository Level: Project-specific patterns
    - Configuration files in the repo
    - You can have multiple instruction files; maybe one for frontend team one for backend team
  3. Organization Level: Company-wide preferences
    - Web-only ([github.com/copilot](https://github.com/copilot)) and Copilot Code Review
  4. Agent Level: Guide GitHub Coding Agent
    - Configuration files in the repo
    - Like when you assign Copilot (GitHub Coding Agent) an issue
- 
- **Precedence:** It'll take suggestions from all levels but more specific will win out
  - **Agent:** Uses all levels + specialized AGENTS.md for autonomous work

Personal preferences for [github.com/copilot](https://github.com/copilot)

# Personal Instructions (in GitHub UI)

**Location:** [github.com/copilot](https://github.com/copilot) settings page

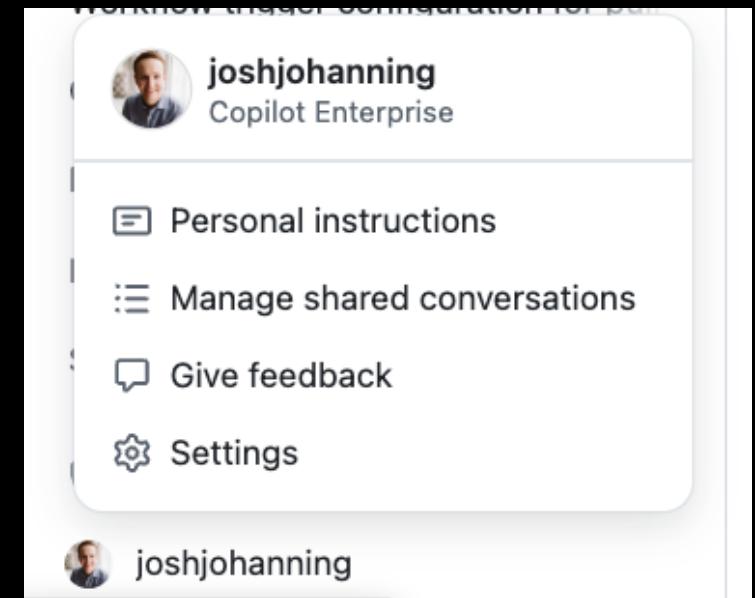
Example:

Your role:

- Senior DevOps Engineer
- Focus on clean, maintainable code

Code guidelines:

- Use JavaScript over TypeScript samples
- Follow functional programming patterns
- Write comprehensive JSDoc comments



**Scope:** Applies to your conversations with Copilot Chat in the GitHub UI

Project conventions

# Repository-Level Instructions Example

**Location:** [github/copilot-instructions.md](#)

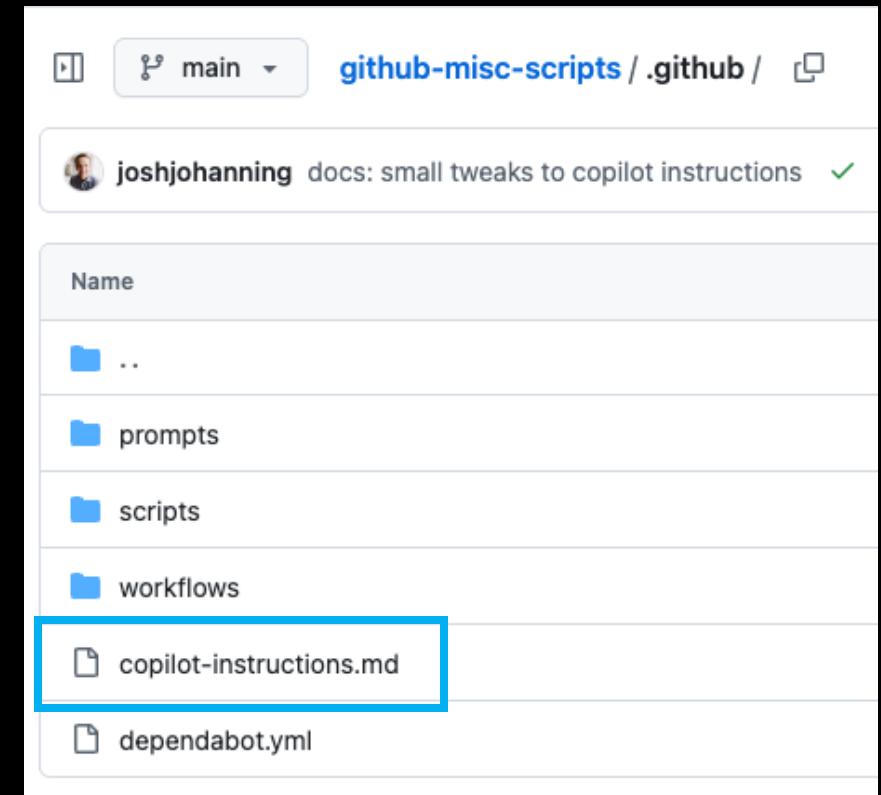
Example:

```
# Copilot Instructions for ProjectX

## Code Style
- Use React functional components with hooks
- State management with Zustand
- CSS with Tailwind utility classes

## Testing
- Jest for unit tests
- React Testing Library for components
- Minimum 80% coverage

## Security
- Never hardcode credentials
- Validate all user input
- Follow OWASP guidelines
```



Tip: In your instruction file, add directory-level breakdown!

# Repository-Level Instructions Example (Advanced)

## Path-specific instructions:

- Create one or more files in: .github/instructions/\*\*/\*.instructions.md

**Example:** .github/instructions/playwright-tests.instructions.md

```
---  
applyTo: "**/tests/*.spec.ts"  
---
```

## Playwright test requirements

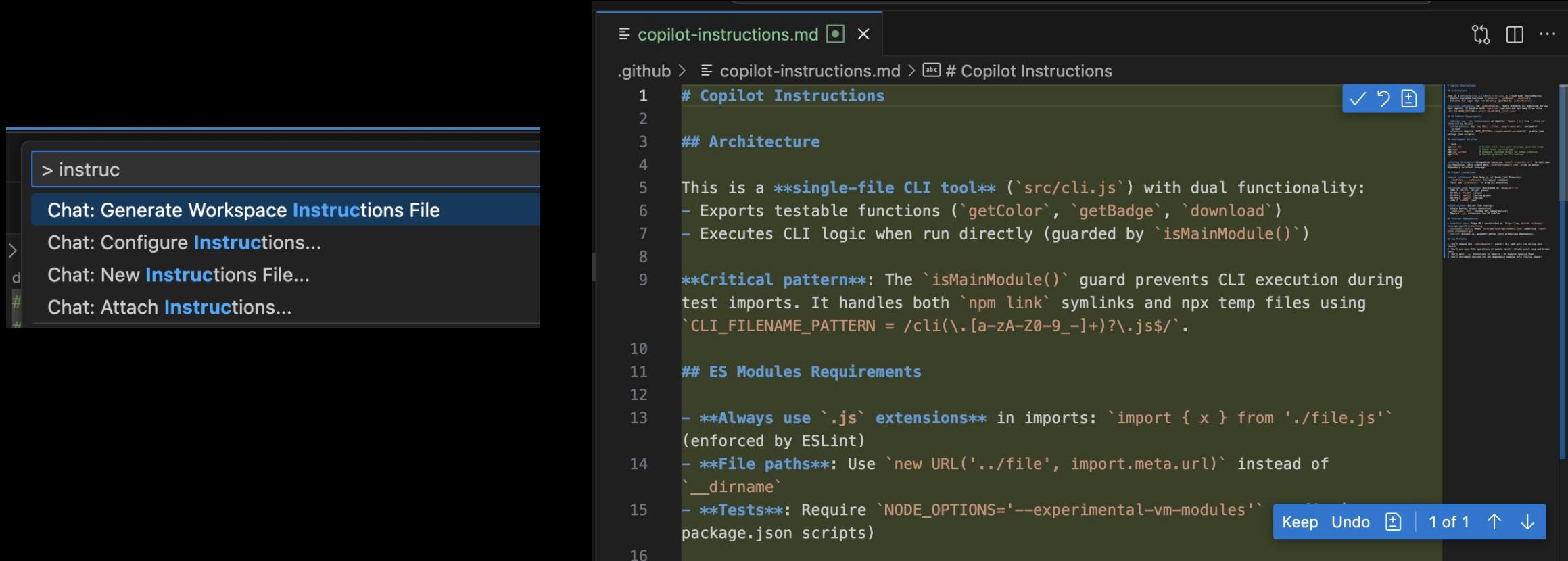
When writing Playwright tests, please follow these guidelines to ensure consistency and maintainability:

• • •

Project conventions

# Repository-Level Instructions

You can use VS Code to help you generate instructions too!



```
# Copilot Instructions

## Architecture

This is a **single-file CLI tool** (`src/cli.js`) with dual functionality:
- Exports testable functions (`getColor`, `getBadge`, `download`)
- Executes CLI logic when run directly (guarded by `isMainModule()`)

Critical pattern: The `isMainModule()` guard prevents CLI execution during test imports. It handles both `npm link` symlinks and npx temp files using `CLI_FILENAME_PATTERN = /cli(\.[a-zA-Z0-9_-]+)?\..js$/`.

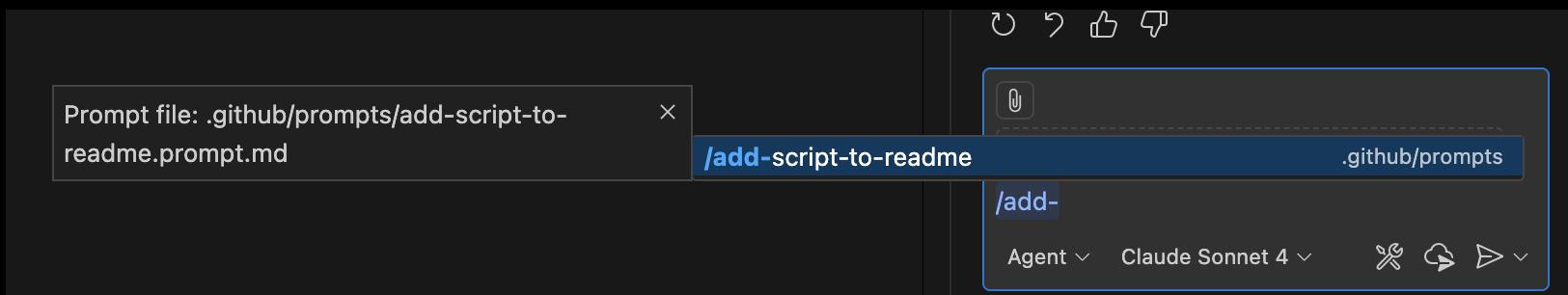
## ES Modules Requirements

- Always use `.js` extensions in imports: `import { x } from './file.js'` (enforced by ESLint)
- File paths: Use `new URL('../file', import.meta.url)` instead of `__dirname`
- Tests: Require `NODE_OPTIONS='--experimental-vm-modules'` package.json scripts)
```

Prompts, or custom commands you can issue to Copilot, can be used with instructions

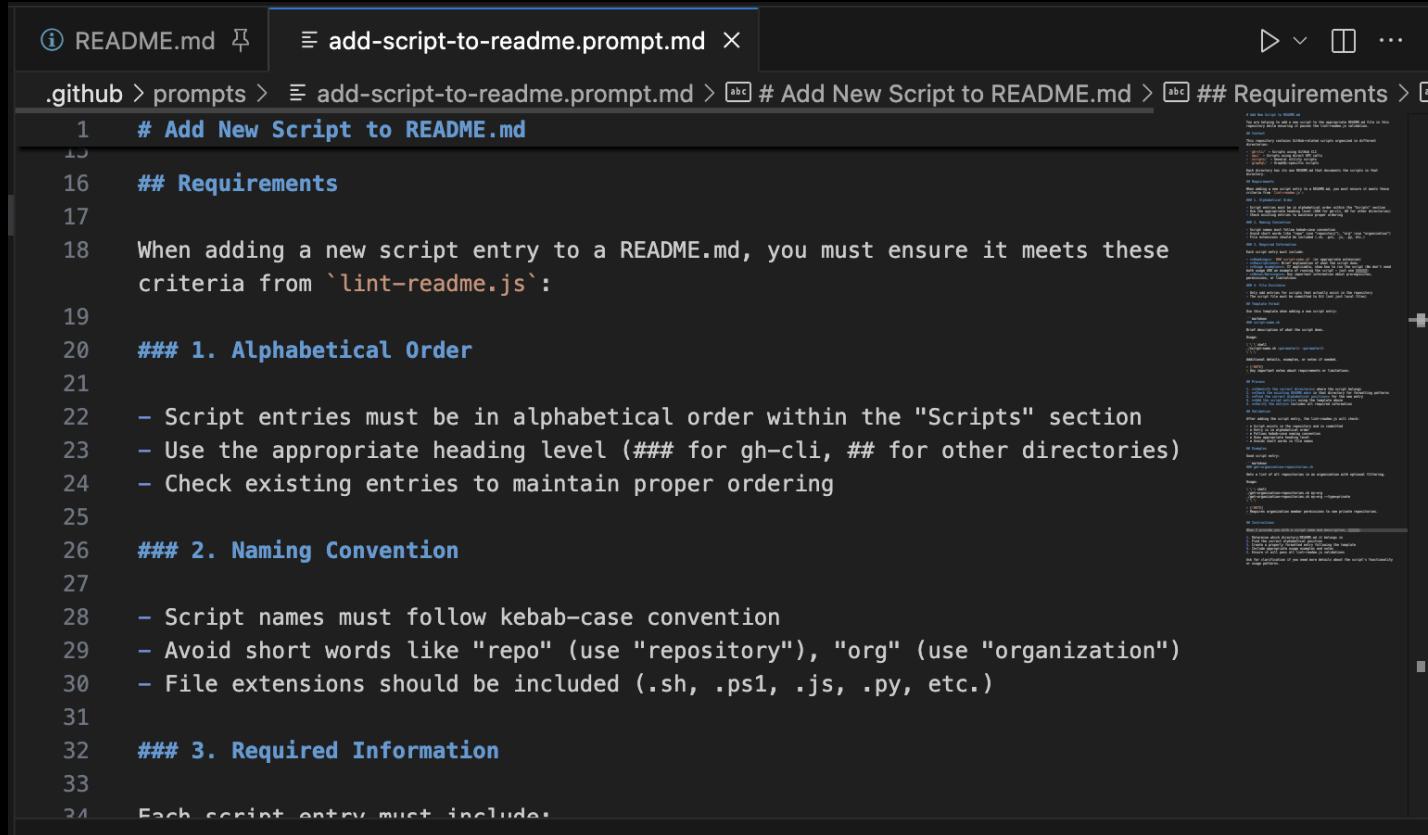
# Prompts / Custom Prompts (Preview)

- Define reusable, version-controlled prompt files in `.github/prompts/`
- Use prompts to standardize workflows – code reviews, API generation, documentation, testing, and more
- Saves time as opposed to typing the same thing every time
- Basically, sharing prompts for the entire time



Prompts, or custom commands you can issue to Copilot, can be used with instructions

# Prompts / Custom Prompts (Preview) Example



The screenshot shows a code editor interface with two tabs: "README.md" and "add-script-to-readme.prompt.md". The "add-script-to-readme.prompt.md" tab is active, displaying a file with the following content:

```
.github > prompts > add-script-to-readme.prompt.md > # Add New Script to README.md > ## Requirements > [Copilot Preview]
```

```
1 # Add New Script to README.md
15
16 ## Requirements
17
18 When adding a new script entry to a README.md, you must ensure it meets these
19 criteria from `lint-readme.js`:
20
21 #### 1. Alphabetical Order
22
23 - Script entries must be in alphabetical order within the "Scripts" section
24 - Use the appropriate heading level (### for gh-cli, ## for other directories)
25 - Check existing entries to maintain proper ordering
26
27 #### 2. Naming Convention
28
29 - Script names must follow kebab-case convention
30 - Avoid short words like "repo" (use "repository"), "org" (use "organization")
31 - File extensions should be included (.sh, .ps1, .js, .py, etc.)
32
33 #### 3. Required Information
34
35 Each script entry must include:
```

A vertical scroll bar is visible on the right side of the code editor window.

Provide generic instructions that will apply to entire organization

# Organization-Level Instructions

**Location:** GitHub Organization Settings (admin required)

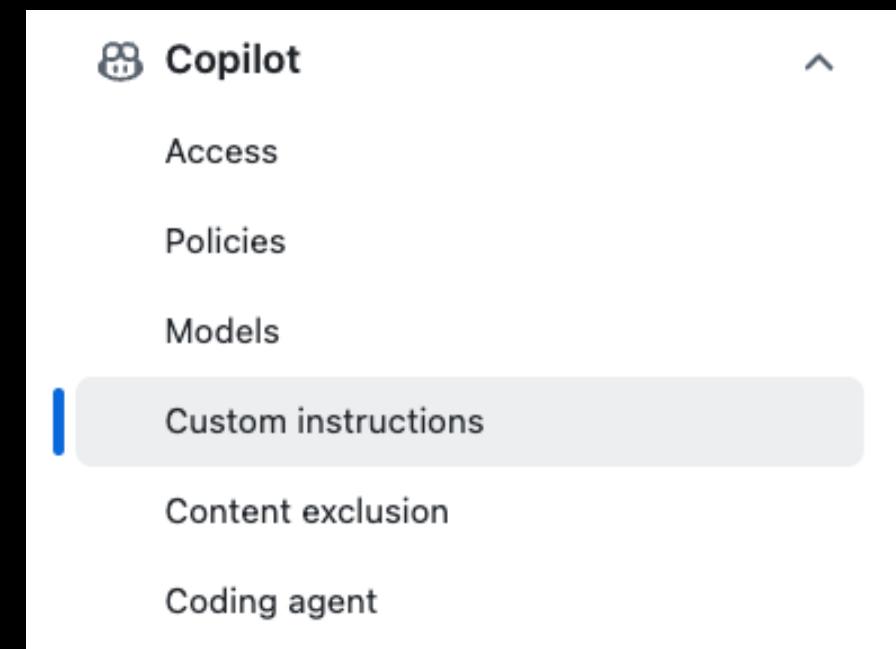
Example:

```
# Org-wide Copilot Coding Review checks

## Security
- Recommend to use auth module for external Auth
- Make sure secrets aren't exposed in logs

## Architecture
- Follow microservices patterns
- Use company message bus
- Ensure CI/CD workflows are updated appropriately

## Dependencies
- Review dependencies to determine if they can be removed because stale/not used
```



Guide Copilot Coding Agent (or any agent)

# Agent-Level Instructions

**Location:** \*\*/AGENTS.md, /CLAUDE.md, GEMINI.md

- Most commonly in root ./AGENTS.md

Example:

```
## Environment Setup
- Install dependencies: `npm install`
- Test: `npm test` (agent verifies changes work)
- Lint: `npm run lint` (agent checks before PR)
- Package: `npm run package` (agent makes sure the project can still be packaged)
```

```
## Development Workflow
- Always run tests before creating PR
- Check existing issues before creating new ones
- Include issue number in commit messages
```

```
## Quality Gates
- Minimum 80% test coverage required
- All tests must pass
- No lint warnings or errors allowed
```

Guide Copilot Coding Agent (or any agent)

# Agent-Level Instructions – why separate?

Spec from OpenAI intentionally keeps it separate to:

- Give agents a clear, predictable place for instructions
- Keep READMEs concise and focused on human contributors
- Provide precise, agent-focused guidance that complements existing README and docs

Tip: Tell Copilot Coding agent how to set up your project:

.github/workflows/copilot-setup-steps.yml

```
# AGENTS.md

## Setup commands
- Install deps: `pnpm install`
- Start dev server: `pnpm dev`
- Run tests: `pnpm test`

## Code style
- TypeScript strict mode
- Single quotes, no semicolons
- Use functional patterns where possible
```

Customize Copilot features in VS Code

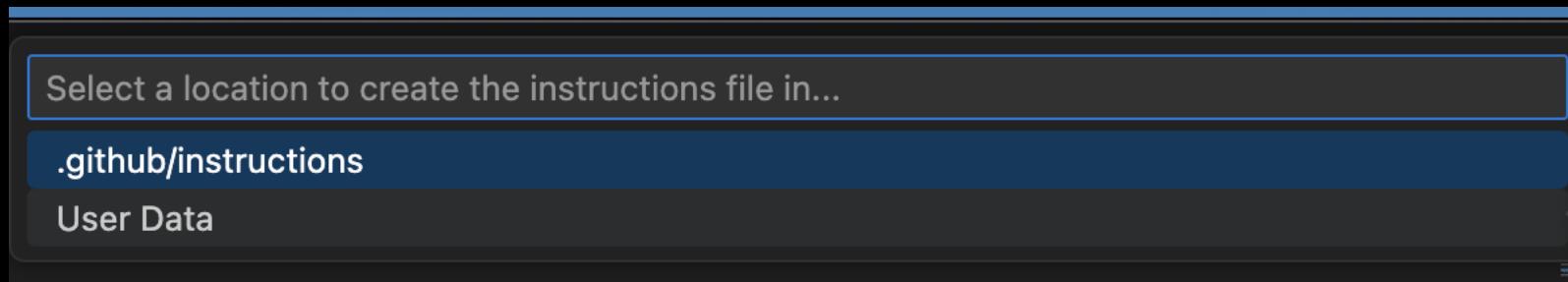
# VS Code: Feature-Specific Instructions

Beyond general instructions, customize specific Copilot features in VS Code (code reviews, commit messages, PR descriptions):

```
{  
  "github.copilot.chat.reviewSelection.instructions": [  
    { "text": "Check for accessibility and WCAG compliance" }  
  ],  
  "github.copilot.chat.commitMessageGeneration.instructions": [  
    { "text": "Use conventional commits (feat/fix/docs) without scope (deps)" }  
  ],  
  "github.copilot.chat.pullRequestDescriptionGeneration.instructions": [  
    { "text": "Always include a list of key changes" }  
  ]  
}
```

This also syncs between VS Code instances if you have settings sync turned on!

# VS Code: User data

A screenshot of a GitHub Actions workflow file named "joshs.instructions.md" in VS Code. The file path is shown at the top: "Users > joshjohanning > Library > Application Support > Code > User > prompts > joshs.instructions.md". The file content is as follows:

```
1 ---  
2 applyTo: '**.yml'  
3 ---  
4  
5 When writing GitHub Actions workflows in YML, provide extra line breaks between  
6 each major section (e.g., between `jobs`, `steps`, etc.) to enhance readability.  
7 Always use 2 spaces instead of 4 spaces for indentation.
```

A small tooltip is visible on the right side of the screen, providing instructions for writing GitHub Actions workflows in YML.

Best practices and tips

# Custom Instructions: How they work together

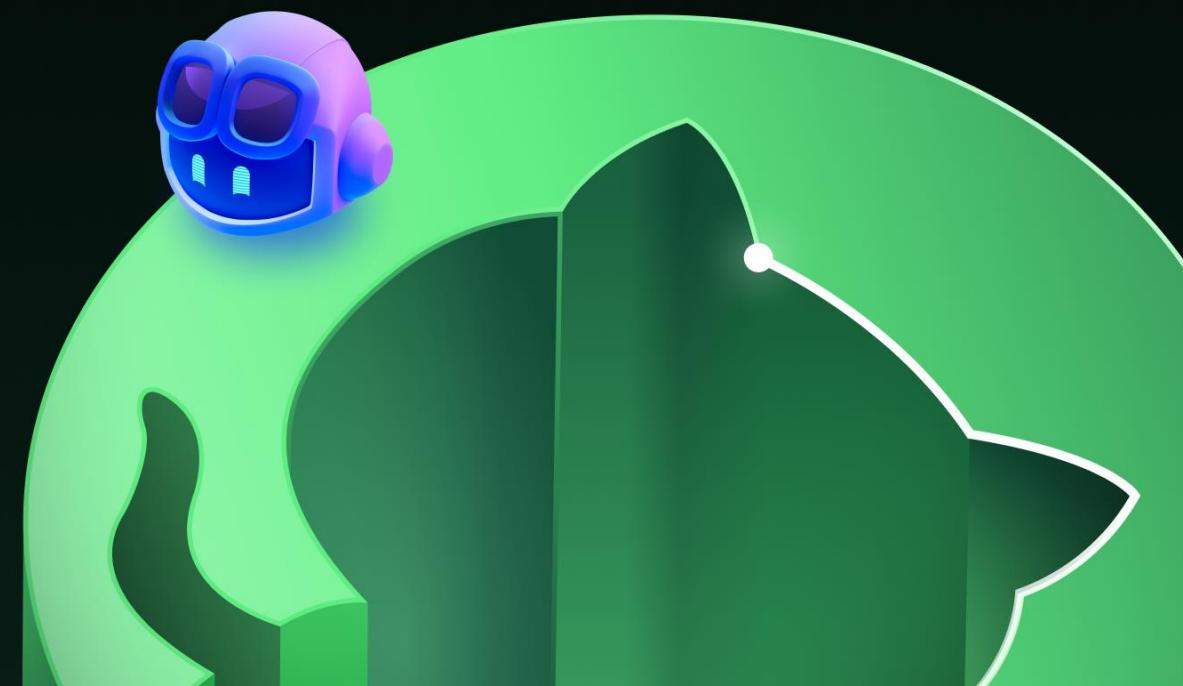
- **Key points:**
  - **All instructions are combined** - they work together, not exclusively
  - **Avoid conflicts** - keep instructions complementary across levels
  - **More specific wins** - path-specific instructions (`.instructions.md`) apply when file matches
- **Best Practice:** Provide enough conventions for Copilot to work locally (in Ask/Edit/Agent mode) AND agentically (Copilot Code Review, Coding Assistant)
- **Tip:** For community-contributed examples of custom instructions and prompts for specific languages and scenarios, see:
  - <https://github.com/github/awesome-copilot>

**Demo: Custom Instructions in Action**

# Exploring Custom Instructions:

1. GitHub Chat in the UI conversation preferences
2. Repository-level instructions
  - Examples
  - Custom prompts
  - awesome-copilot
3. Organization-level instructions
4. Agent instructions
5. VS Code feature settings

**Code that matches your conventions!** 🤖



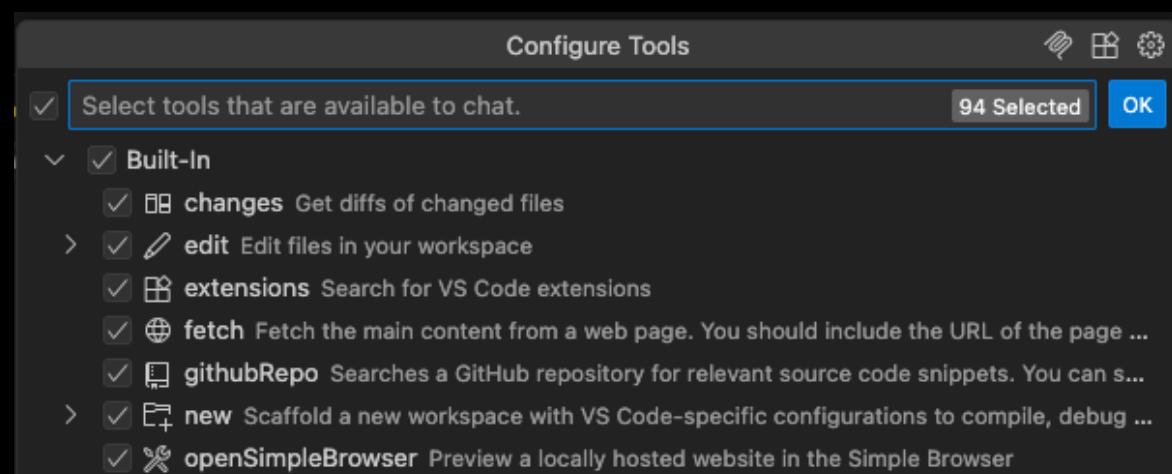
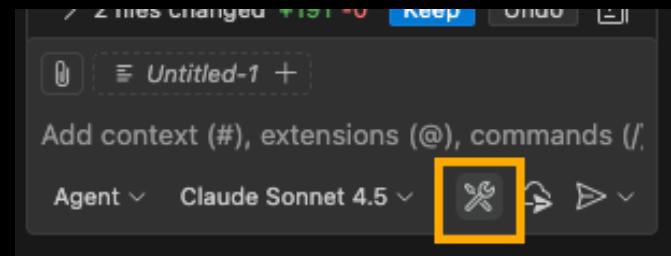
# Part 3: Understanding Tools in Copilot

Functions AI can invoke

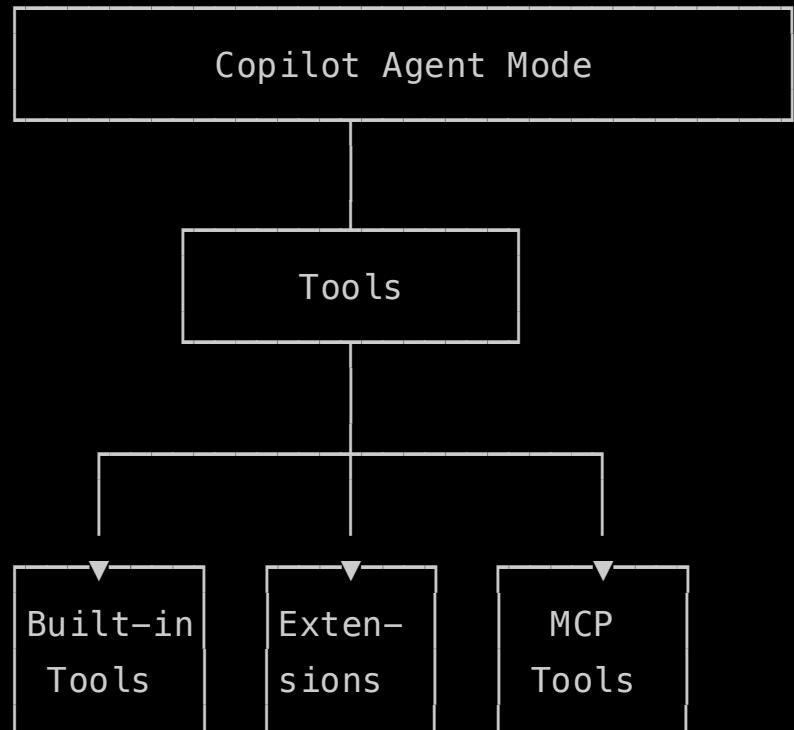
# What are Tools in Copilot?

**Tools** are functions that Copilot can call to take actions or gather information:

- **List files** in a directory
- **Edit files** in your workspace
- **Run terminal commands** (build, test, deploy)
- **Search code** across your codebase
- **Create GitHub issues and PRs**
- **Query APIs** and databases



# Types of Tools

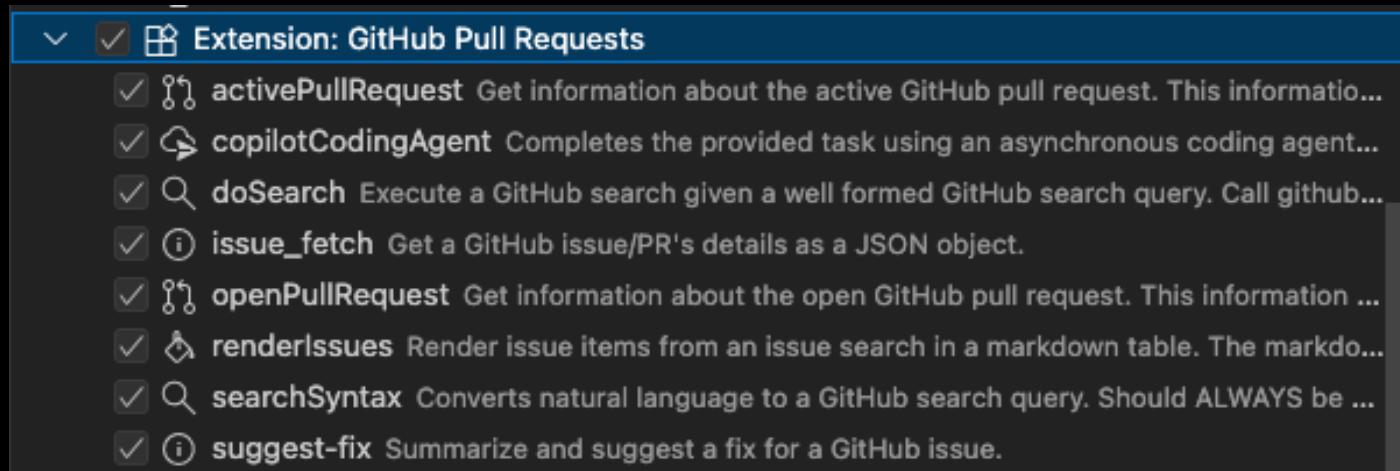


- **Built-in Tools:** VS Code core capabilities (file edits and creating files and directories, running terminal commands, etc.)
- **Extension Tools:** Added by extensions (GitHub PR, Azure, etc.) - **No MCP needed!**
- **MCP Tools:** Your custom integrations (docs, APIs, databases)
  - Think of how these can be used in the upcoming sections!

Tools without MCP!

# Example: GitHub Pull Request Extension Tools

- **The Bridge:** Extensions like this give Copilot powerful capabilities **without any MCP setup**
- Tools will be selected automatically based on your query, can use #ToolName to specifically select



#activePullRequest how many reviewers does this have?

activePullRequest

> Used 1 reference

Based on the active pull request data, this PR has **2 reviewers** who have approved it:

1. **tspascoal** - Approved
2. **kenmuse** - Approved (with comment "LGTM!")

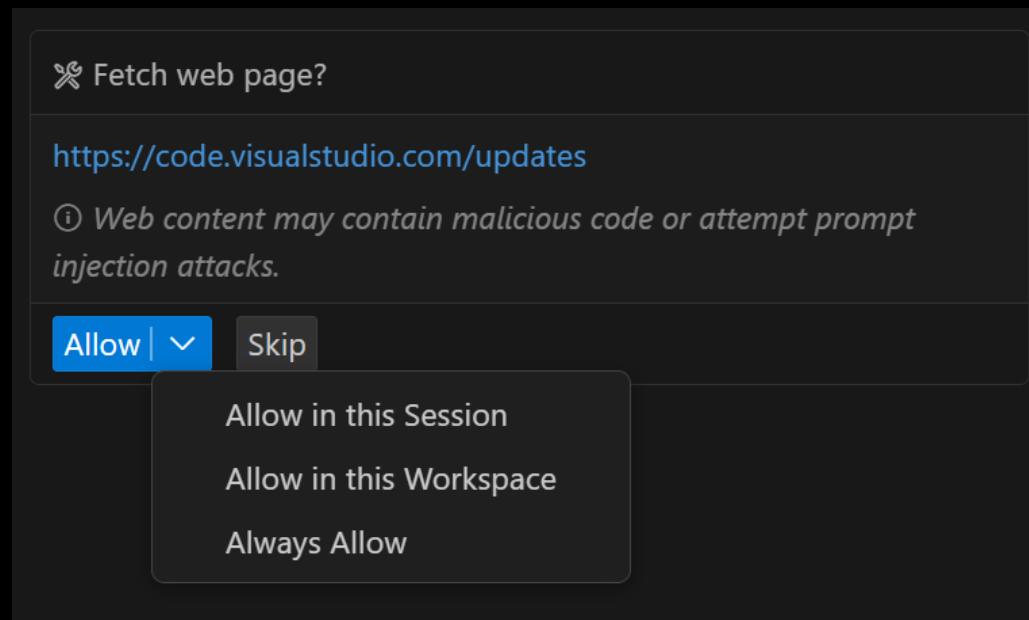
There are also automated review comments from **copilot-pull-request-reviewer** (which generated 3 comments that have all been resolved), but those are automated reviews and not counted as human reviewers.



You can approve trusted tools in workspace or always

# Tools – Approval Prompt

Asks for you to trust the tool before running – prevents running unsafe tools or unintentional prompt injection

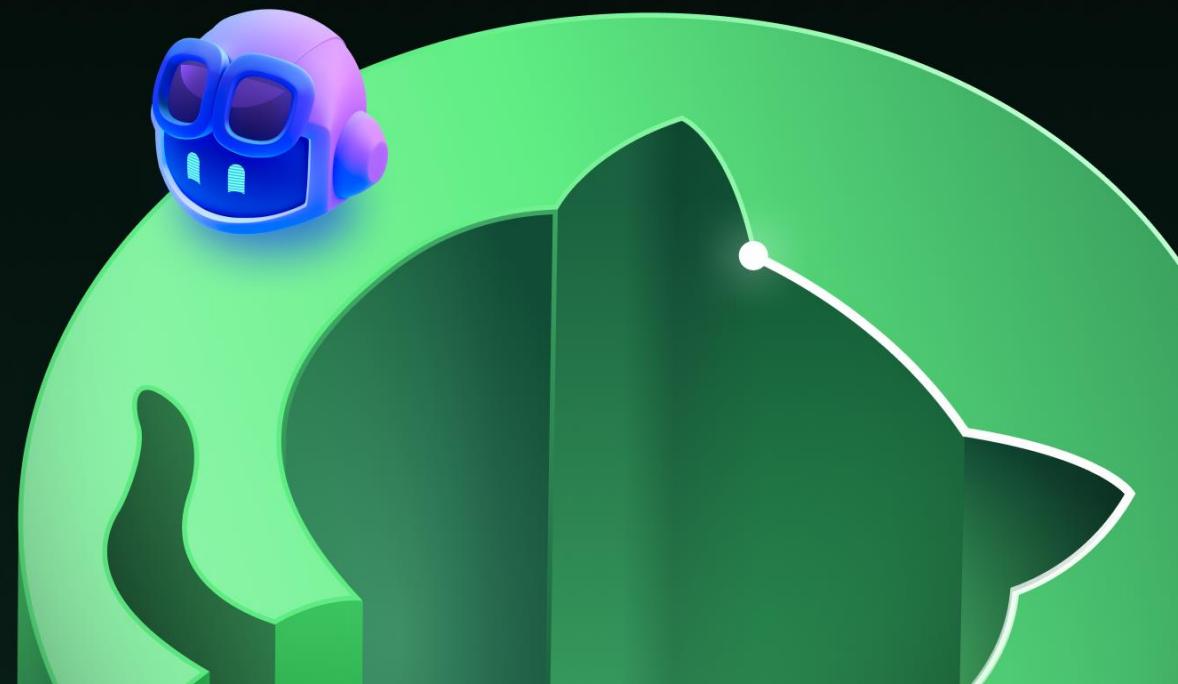


# Part 4: The Model Context Protocol (MCP)

What is MCP?

**Before diving into  
MCP, let's recap  
how we got here**

Before there was MCP, there were  
Copilot Extensions...

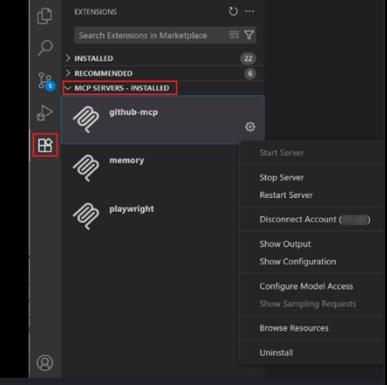




## Copilot Extensions in Preview

May 2024

Launched with an initial set of partners in our partner program, like Docker, LaunchDarkly, and Microsoft Azure and Teams



## Anthropic launches MCP

November 2024

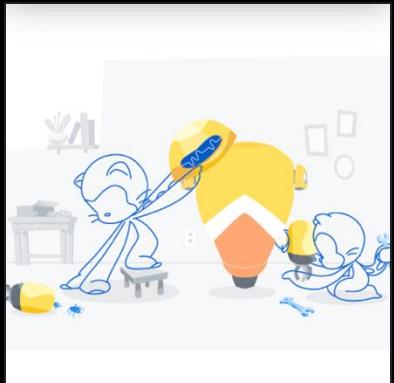
Debut as an open standard for connecting AI assistants to data systems (code, business systems, etc.)



## GA: Copilot Extensions

February 2025

Platform open for anyone to create public or private extensions to be able to use Copilot to access external systems



## GA: MCP support in VS Code

July 2025

VS Code 1.102 fully supports MCP (in preview for Visual Studio in June)

## GitHub MCPs + Marketplace

April–September 2025

April: GitHub local MCP server *preview*

June: GitHub remote MCP server *preview*

Sept: GitHub remote MCP server GA, MCP Marketplace debut

## Extension Sunset, Retirement

September 2025 – November 2025

In favor of MCP – with the writing on the wall with the GitHub MCP for a while now! Extensions will be disabled on November 10.

# The now sunset Copilot Extension Marketplace

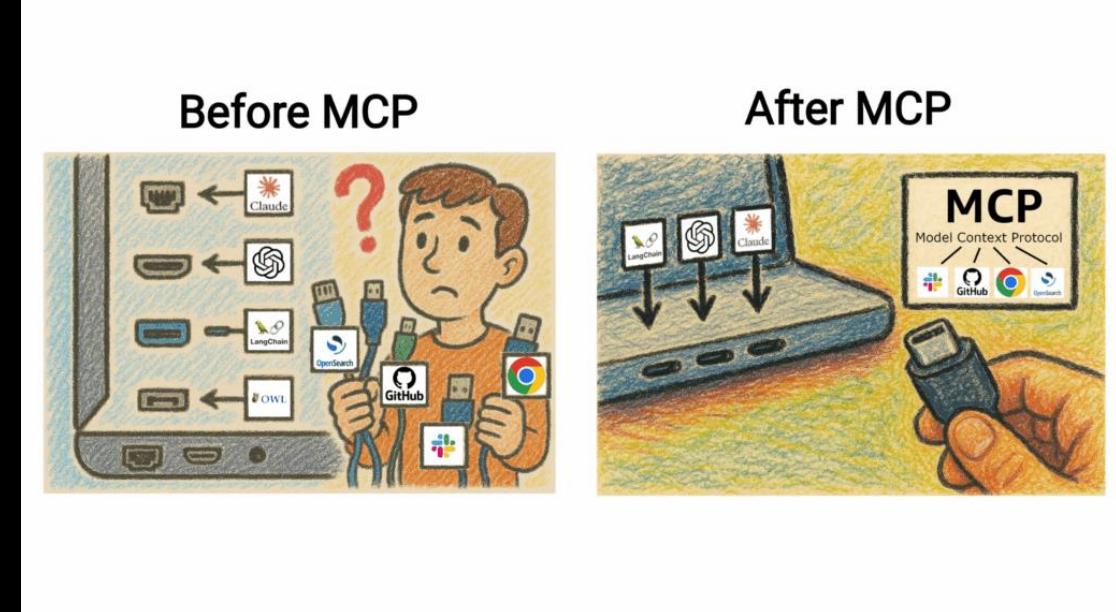
The screenshot shows a browser window for [github.com](https://github.com) displaying the Copilot Extension Marketplace. A yellow warning bar at the top states: "Warning: We are deprecating GitHub Copilot Extensions on November 10, 2025, in favor of the Model Context Protocol (MCP). You can read more about this change in our [changelog.post](#)." The left sidebar has a "Copilot" section selected, showing links for "Featured", "Copilot", "Models", "Apps", "Actions", and "Create a new extension". The main content area is titled "Copilot Extensions" and describes how to "Extend Copilot capabilities using third party tools, services, and data". It features a search/filter bar with dropdowns for "Filter: All", "By: All creators", and "Sort: Popularity". Below are cards for nine extensions:

- PerplexityAI** (Copilot) - Perplexity answers questions as you code by searching the web.
- Docker for GitHub Copilot** (Copilot) - Learn about containerization, generate Docker assets and analyze project vulnerabilities in GitHub Copilot.
- Models (GitHub)** (Copilot) - Copilot Extension to connect and chat with GitHub Models.
- Stack Overflow** (Copilot) - Get answers to your most complex coding questions right where you're already working.
- Mermaid Chart** (Copilot) - Provides advanced and powerful diagramming and visualization to GitHub Copilot Chat.
- Microsoft 365 Agents Toolkit** (Copilot) - Chats with GitHub Copilot extension for Microsoft 365 Agents. Toolkit to build applications and agents for Microsoft 365.
- GitBook for GitHub Copilot** (Copilot) - Leverage your GitBook documentation to answer questions, providing instant responses in your workflow.
- ReadMe API** (Copilot) - Ask questions about the ReadMe API and get help with code, directly in VS code.
- Agentic Search Ai** (Copilot)
- Product Science** (Copilot)

# What is MCP?

**Model Context Protocol (MCP)** is an open protocol that standardizes how AI applications connect to data sources and tools.

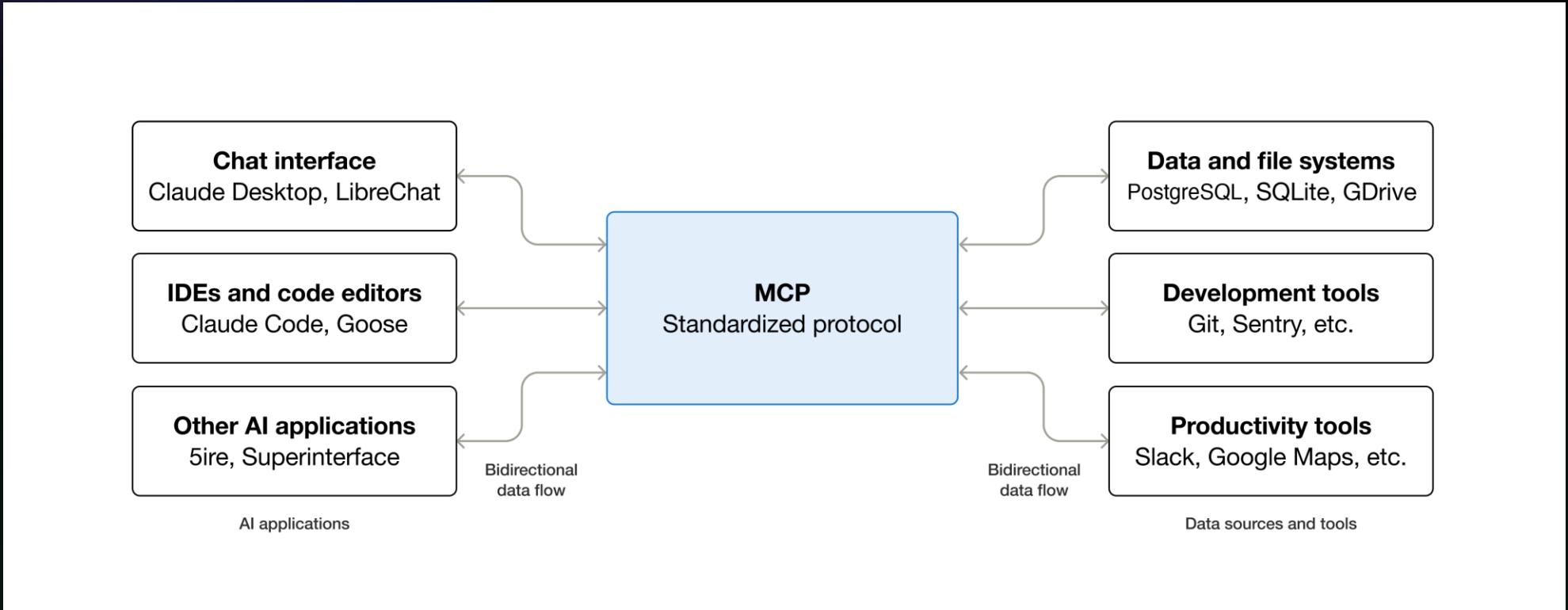
- Created by Anthropic (makers of Claude)
- Open-source and vendor-neutral
- Designed for LLM integration
- Extensible architecture
  - For the techies – two main options:
    - JSON-RPC over stdio (local, simplest)
    - Streamable HTTP transport (remote)



“

Think of MCP like a USB-C port for AI  
applications

[modelcontextprotocol.io](http://modelcontextprotocol.io)



# Why MCP Matters

## Before MCP:

- Limited context windows (*developers constantly hitting token limits*)
- Manual copy-paste workflows (*tedious context switching*)
- Disconnected from live data (*stale information, outdated assumptions*)
- Custom integrations per tool (*brittle, maintenance-heavy*)

## With MCP:

- Dynamic context injection (*AI knows your codebase state when accessing external data*)
- Real-time data access (*always up-to-date information*)
- Standardized connections (*write once, use everywhere*)
- Reusable and sharable servers (*share publicly to customers or privately within your team*)

“

MCP is the “HTTP protocol” of the AI world

We will talk more about building MCPs more later!

# MCP Server Communication Models

<u>Context</u>	<u>Transport</u>	<u>Used For</u>	<u>Pros</u>	<u>Cons</u>
Local	JSON-RPC over STDIO	Local dev tools, VS Code extensions, sharing w/in small teams	Fast, simple, no network setup	Only works locally
Remote	Streamable HTTP (SSE/WebSocket)	Hosted MCPs, enterprise integrations, marketplace MCPs	Works across network, supports auth & streaming	More overhead, latency

*For now, just understand there are local and remote MCP servers*

What Can MCP Servers Do?

# MCP Server Capabilities

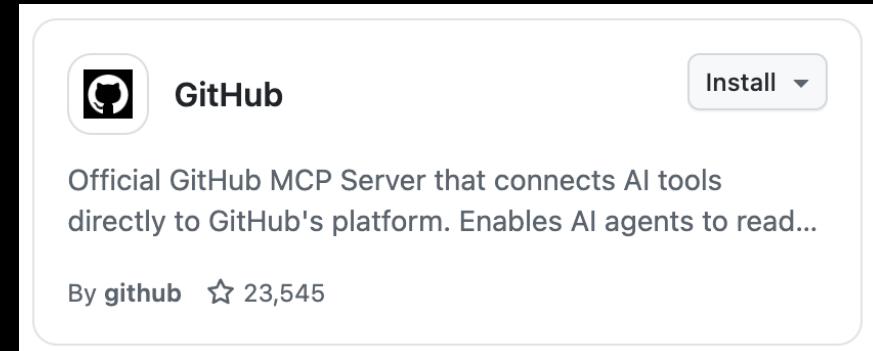
1. **Resources:** Expose data (files, API responses, DB records) (*nouns*)
2. **Tools:** Provide callable functions (search, create, update) (*verbs*)
3. **Prompts:** Offer reusable prompt templates
4. **Sampling:** Implement agentic behaviors by enabling LLM calls to occur nested inside other MCP server features

# Part 5: Building Custom Context Providers (MCPs)

Where MCP shines

# Use Cases for Custom Context Providers

- **Documentation Systems:** Connect Confluence, Notion, internal wikis
- **Issue Trackers:** Query Jira, Azure DevOps, GitHub to integrate requirements
- **Source Control & SDLC:** Code, PRs, issues, projects, actions in GitHub 
  - *GitHub's remote MCP server is now GA!*
- **Databases:** Query production/staging data
- **APIs:** Internal services and microservices
- **Code Analysis:** Static analysis tools, test coverage
- **Metrics:** Application performance, logs



Most commonly we will use Tools, but it's good to know about the others too!

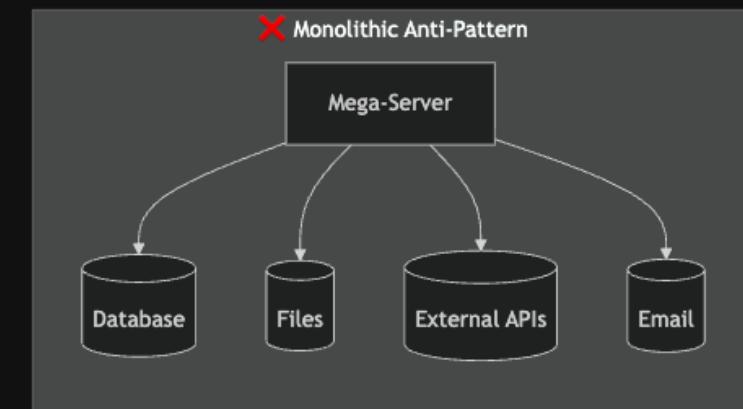
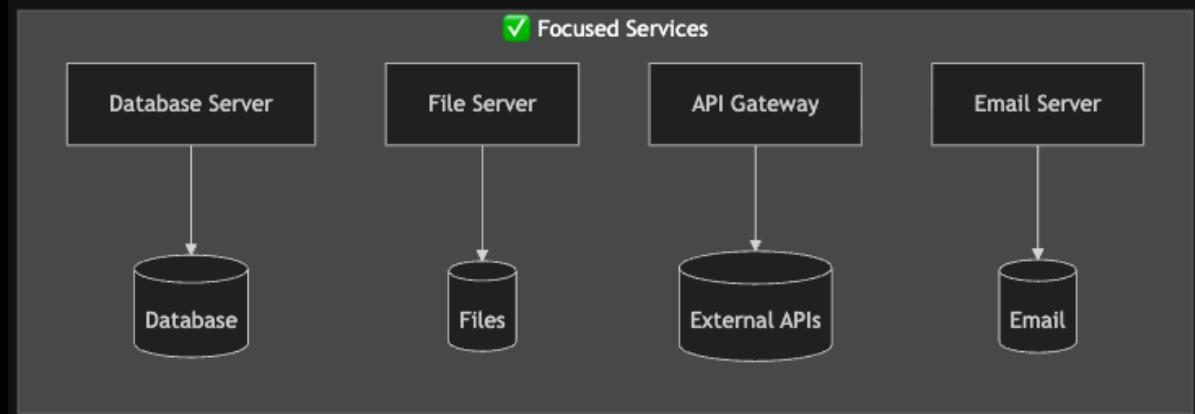
# Core MCP Server features

- **Tools**
  - Functions that your LLM can actively call, and decides when to use them based on user requests
  - Examples: create pull request comment, create calendar event, search flights
- **Resources**
  - Passive data sources that provide read-only access to information for context
  - Examples: API schemas, databases, file contents/knowledge bases
- **Prompts**
  - Pre-built instruction templates that tell the model to work with specific tools and resources
  - Examples: /create-pr-with-summary, /build-trip-itinerary, /summarize-my-meetings

Single responsibility principle

# Architectural Design Principle

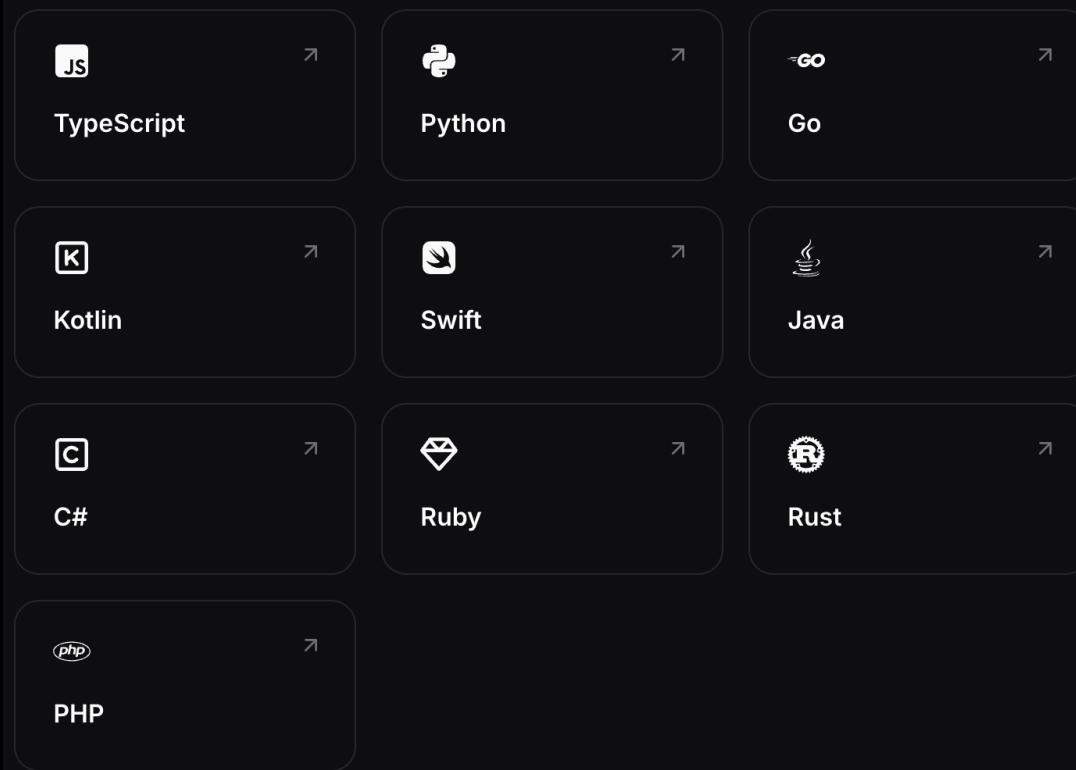
- Design your MCP server with a single focus in mind
  - Think: microservices
- Benefits:
  - Maintainability
  - Scalability
  - Reliability
  - Isolated team ownership



Supported SDKs for nearly any language!

# Building your first MCP Server - SDKs

## Available SDKs



## Basic Structure (JavaScript)

# Building Your First MCP Server

```
import { Server } from "@modelcontextprotocol/sdk/server/index.js";
import { StdioServerTransport } from "@modelcontextprotocol/sdk/server/stdio.js";
```

```
const server = new Server(
```

```
{
  name: "my-context-provider",
  version: "1.0.0",
```

```
},
```

```
{
```

```
  capabilities: {
    resources: {},
    tools: {},
```

```
},
```

```
,
```

```
);
```

# Implementing Resources

```
// List available resources
server.setRequestHandler(ListResourcesRequestSchema, async () => {
  resources: [
    {
      uri: "docs://architecture/overview",
      name: "Architecture Documentation",
    },
  ],
}) );
```

```
// Read resource content
server.setRequestHandler(ReadResourceRequestSchema, async (request) => {
  const content = await fetchDocumentation(request.params.uri);
  return { contents: [{ uri: request.params.uri, text: content }] };
});
```

# Implementing Tools

```
// Define available tools
server.setRequestHandler(ListToolsRequestSchema, async () => ({
  tools: [
    {
      name: "search_docs",
      description: "Search internal documentation",
      inputSchema: {
        /* ... */
      },
    },
  ],
}) );
```

```
// Handle tool calls
server.setRequestHandler(CallToolRequestSchema, async (request) => {
  const results = await searchDocs(request.params.arguments.query);
  return { content: [{ type: "text", text: results }] };
});
```

Great utility for working with and debugging local and remote MCPs!

# Using MCP Inspector to verify/debug

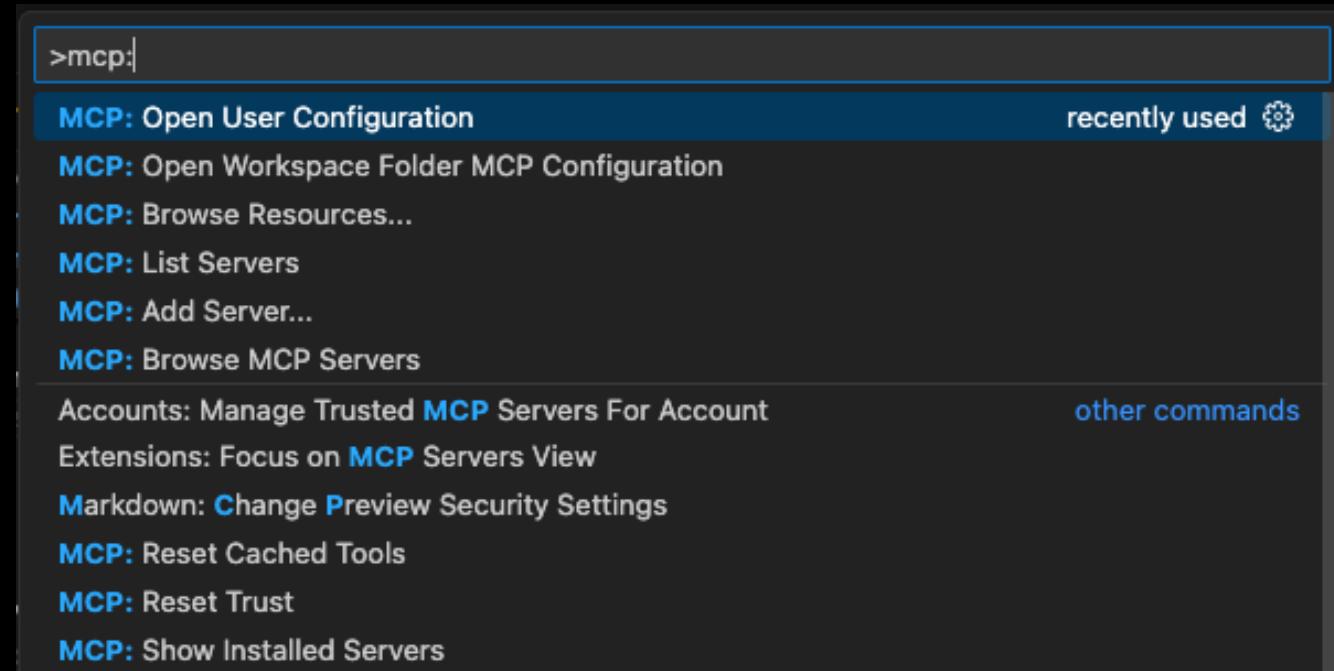
Think of the MCP Inspector as Swagger UI or Postman but for MCP servers instead of Rest APIs

```
npx @modelcontextprotocol/inspector node index.js
```

The screenshot shows the MCP Inspector application window. On the left, a sidebar contains configuration fields: 'Transport Type' set to 'STDIO', 'Command' set to 'node', and 'Arguments' set to 'index.js'. Below these are buttons for 'Environment Variables', 'Server Entry', and 'Servers File'. The main area has a top navigation bar with tabs: Resources, Prompts, Tools (which is selected), Ping, Sampling, Elicitations, Roots, and Auth. The 'Tools' tab section displays a search bar and two buttons: 'List Tools' and 'Clear'. It lists two tools: 'search\_docs' (described as 'Search through documentation files for specific content') and 'get\_weather' (described as 'Get current weather for a city using OpenWeatherMap API. Supports city names, 'City, Country' format (e.g., 'London, UK'), or 'City, State, Country' for US cities (e.g., 'Madison, Wisconsin, US')'). A modal window titled 'Select a tool' is open on the right, with the message 'Select a tool from the list to view'.

# Configuring MCPs in VS Code

```
"servers": {  
    "github": {  
        "type": "http",  
        "url": "https://api.githubcopilot.com/mcp/"  
    },  
    "techorama-demo": {  
        "command": "node",  
        "args": ["/path/to/local/mcp/server/index.js"],  
        "env": {  
            "MY_SECRET": "${input:mySecret}"  
        }  
    },  
    "inputs": [  
        {  
            "id": "mySecret",  
            "type": "promptString",  
            "description": "mySecret token!",  
            "password": true  
        }  
    ]  
}
```



Tip: You can create a `.vscode/mcp.json` file in your workspace and commit it!

# Best Practices for Context Providers

## ✓ Do:

- Use **clear, descriptive tool/resource names** (Copilot uses to decide when to invoke)
- Implement proper error handling with helpful messages
- **Use VS Code's secure credential storage** ( `${input:variable}`  pattern)
- Return focused, relevant data (not entire databases)
- Use streaming responses for large payloads
- **Containerize MCPs** - don't give it full access to the file system!!!
- Test with MCP Inspector before deploying
  - `npx @modelcontextprotocol/inspector node index.js`

*There's a whole slew of best practices – see my resources link at the end*

# Best Practices for Context Providers

## ✗ Don't:

- **Hardcode API keys or secrets in configuration**
- **Expose sensitive data without authentication**
- Return massive payloads that slow down responses
- Run servers in Docker detached mode (breaks stdio communication)
- **Trust user input without validation**
- **Allow highly privileged commands** (`sudo`, `rm -rf`) to run
- Ignore timeout configuration (servers can hang indefinitely)

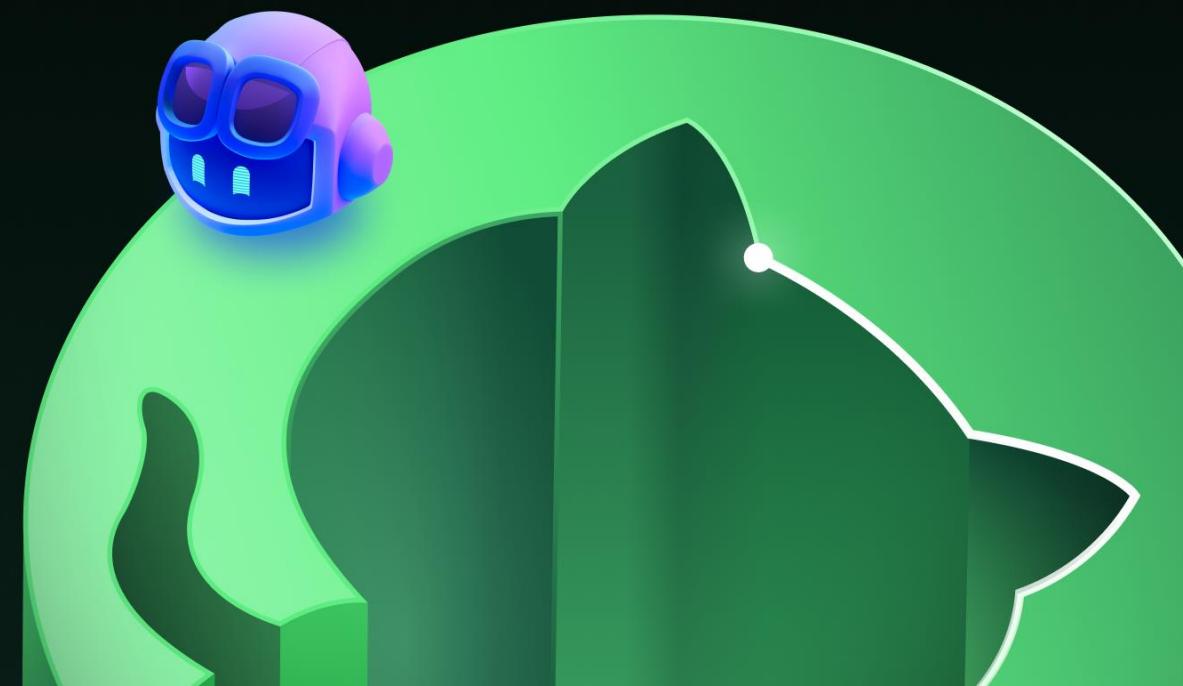
*There's a whole slew of best practices – see my resources link at the end*

Demo: MCP in Action

# We'll explore a custom MCP server that:

1. Connects to a documentation system
2. Exposes docs as resources
3. Provides search functionality
4. Adds weather API lookup
5. Demonstrates MCP chaining with another MCP

Then see it work with Copilot in real-time! 🤖



# Part 6: MCP Server Hosting, Registries, and Policies

Two transport patterns

# Local vs Remote MCP Servers

## Local:

- Runs on developer machine
- Process spawned by VS Code
  - You should be containerizing ☺
- Uses standard input/output
- Best for: Personal tools, fast iteration, debugging

## Remote:

- Deployed and hosted like any other software
- Offloads computational load to remote server
- Centralized context and consistency
- Best for: Shared resources, enterprise data, proper logging, and telemetry gathering

Where to host your HTTP MCP servers

# Remote MCP Server Hosting Options

Think like you're publishing an API - you can host it virtually anywhere!

- **Serverless Functions:**
  - Azure Functions, AWS Lambda, Google Cloud Functions
  - Best for: Lightweight servers, sporadic usage (cold starts can affect latency)
- **Container Services:**
  - Azure Container Apps, AWS ECS/Fargate, Google Cloud Run
  - Best for: Production workloads, consistent performance (easy scaling, good monitoring)
- **Kubernetes:**
  - Full orchestration control
  - Best for: Enterprise scale, high availability (complex setup, overkill for small teams)
- **Self-Hosted:**
  - Your own infrastructure
  - Best for: Sensitive data, compliance requirements (full control, more maintenance)

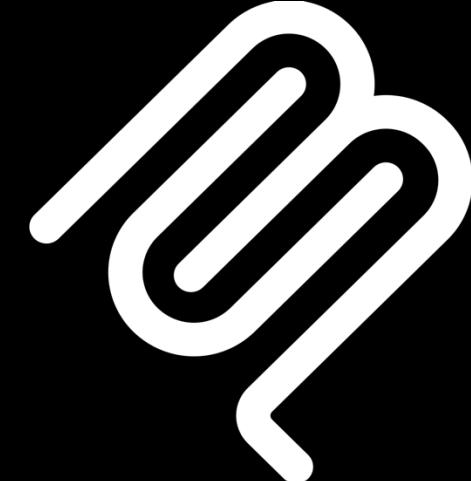
Production readiness checklist

# Deployment/hosting Best Practices

If you build and deploy software, these should look familiar ☺

- **Security:**
  - Validate inputs, sanitize outputs, no exposed secrets
- **Performance & Reliability:**
  - Health checks + timeouts (30s max)
  - Rate limiting + caching for frequently accessed data
- **Observability:**
  - Log tool calls with context (what, when, who)
  - Monitor errors, set alerts, track usage patterns
- **Safe Deployments:**
  - **Validate with MCP Inspector first**
  - Rolling updates
  - Versioned

# MCP Registries



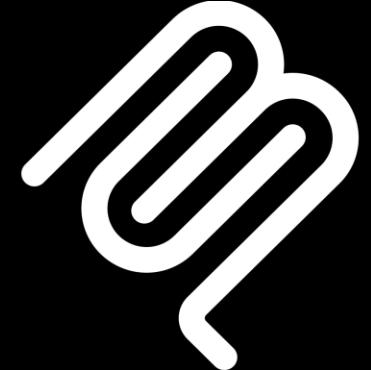
- **What is an MCP registry?**
  - Central directory of available MCP servers
  - Discover servers built by your organization or community
  - Simplify server distribution and update management
- **GitHub has a Public MCP registry:**
  - [github.com/mcp](https://github.com/mcp)
  - Curated list from leading partners and open-source community
  - Servers sorted by GitHub stars and community activity
- **Internal Registries:**
  - Create your own internal catalog for your organization
  - Add proprietary/internal-only servers
  - Control governance and compliance with organization/enterprise settings in GitHub

# GitHub MCP Registry

The screenshot shows a dark-themed browser window displaying the GitHub MCP Registry. The URL bar at the top shows "github.com". Below the bar is a search input field with the placeholder "Search MCPs" and a magnifying glass icon. The main content area is titled "All MCP servers 44". It displays a grid of 12 MCP server cards, each with a small icon, the name of the server, a brief description, the developer, and a star rating.

MCP Server	Description	Developer	Stars
Markitdown	Convert various file formats (PDF, Word, Excel, images, audio) to Markdown.	By microsoft	81,735
Context7	Get up-to-date, version-specific documentation and code examples from any library or framework.	By upstash	33,998
GitHub	Official GitHub MCP Server that connects AI tools directly to GitHub's platform. Enables AI agents to read...	By github	23,655
Playwright	Automate web browsers using accessibility trees for testing and data extraction.	By microsoft	21,971
Serena	Semantic code retrieval & editing tools for coding agents.	By oraios	14,340
Chrome DevTools	Lets your coding agent (such as Gemini, Claude, Cursor or Copilot) control and inspect a live Chrome browser.	By ChromeDevTools	11,240
Firecrawl	Extract web data with Firecrawl	By firecrawl	4,728
Unity	Control the Unity Editor from MCP clients via a Unity bridge + local Python server.	By CoplayDev	3,505
Notion	Official MCP server for Notion API	By makenotion	3,324
Azure	The Azure MCP Server, bringing the power of Azure to your agents.		
Terraform	Seamlessly integrate with Terraform ecosystem, enabling advanced automation and interaction capabilities for...		
Microsoft Learn	Enables clients like GitHub Copilot and other AI agents to bring trusted and up-to-date information directly from...		

"The MCP Registry"



# From MCP: The MCP Registry

In partnership from MCP creators and other maintainers - including GitHub

- Public **catalog and API** for discovering Model Context Protocol (MCP) servers
- **Open source and extensible** – anyone can build compatible sub-registries
- Designed for **discoverability and standardization** across the MCP ecosystem
- Supports **public and private registries** with shared schema and governance
- Currently in **preview** – feedback and community contributions encouraged

<https://github.com/modelcontextprotocol/registry>

Specify a MCP registry for organization-wide control

# Internal MCP registry and allowlist Insiders

- Configuring MCP server access in an Enterprise/organization
  - Coming soon to other IDEs!
  - Safely curate a registry (hosted somewhere) of approved MCP servers for your users

The screenshot shows the MCP registry configuration section within the Copilot settings. It includes fields for the MCP registry URL, a dropdown for restrict MCP access to registry servers, and links for documentation.

**MCP servers in Copilot**  
If enabled, users can configure Model Context Protocol (MCP) servers (including third-party servers) for Copilot in all Copilot editors and Coding Agent. Enabled

**MCP registry URL (optional)**  
URL for a [specification-compliant](#) MCP registry. MCP servers listed in this registry will be visible to members. Note that the MCP registries are currently supported in VS Code only, with support for all Copilot IDEs coming soon.  
 Save

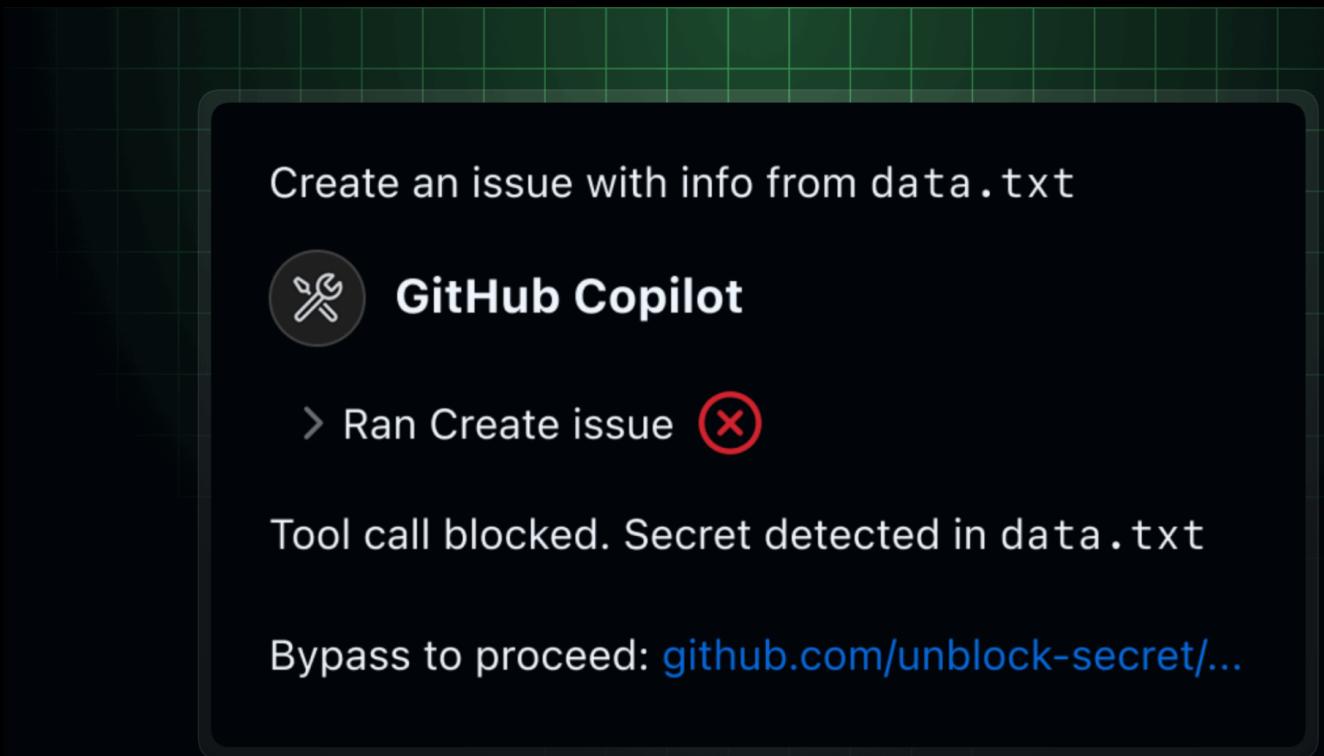
**Restrict MCP access to registry servers**  
Control which MCP servers are allowed based on your registry configuration. Allowlisting is currently only supported on VS Code Insiders. Allow all

[View docs on MCP registry allow lists.](#)

This helps prevent accidentally LEAKING secrets to a malicious repo in GitHub

## GitHub MCP Server: Secret scanning, push protection

- We scan all tool call inputs in public repositories
- If an exposed secret is detected, call is blocked by default
- This protects prompt injection – public instructions/readmes can trick agents into pasting credentials into MCP tool calls
- By inspecting data flowing to and from public repositories, this cuts out a common exfiltration path
- Support for private repositories with a GitHub Secret Protection license is coming soon



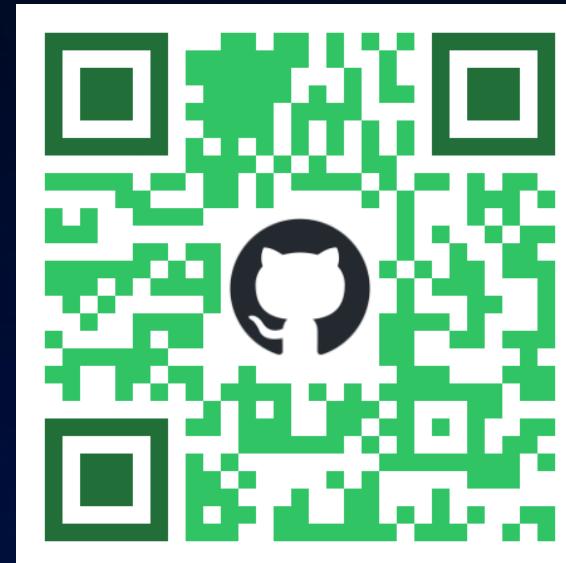
What takeaways do we have?

## Recap

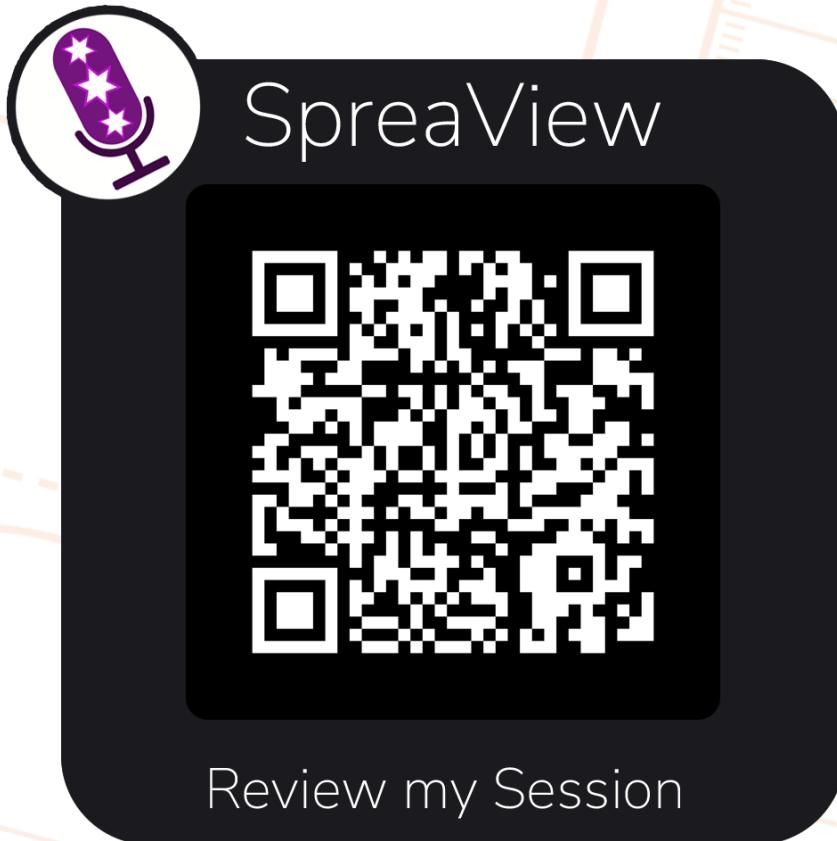
- Use **custom instructions!**
  - Recommend repository-level custom instructions – path-specific instructions good too!
- **Tools!** Some extensions have tools (like the GitHub Pull Request extension)
- **MCPs** – you now know what they are!
  - Universal protocol for AI assistants
- Install the **GitHub Remote MCP server**
- Explore the **GitHub MCP registry**
  - The Playwright MCP server is AWESOME for navigating websites interactively and using AI to analyze and query against
  - Plug for the Azure and Microsoft Learn MCP server as well
- More **MCP Server policies** are coming soon for administrators

# Resources / Slides

[gh.io/josh-copilot-talk](https://gh.io/josh-copilot-talk)



# Survey



# Slides / resources





# Thank you

