

# The Magic of MCP

**Mark Good** - Founder - *AI Force Training*

**Vernon Keenan** - Founder & Senior Industry Analyst - *Keenan Vision*

**Chris Pearson** - Director of Research Programs - *Keenan Vision*

July 16th, 2025

# Agenda

- Why Model Context Protocol (MCP) Matters Now
- Getting Started with MCP: Resources, Risks & Recommendations
- Installing & Using 3rd Party MCP Servers
- MCP's Role in the Future of DevOps for Salesforce
- MCP and AI Force Training: What It Unlocks for Teams



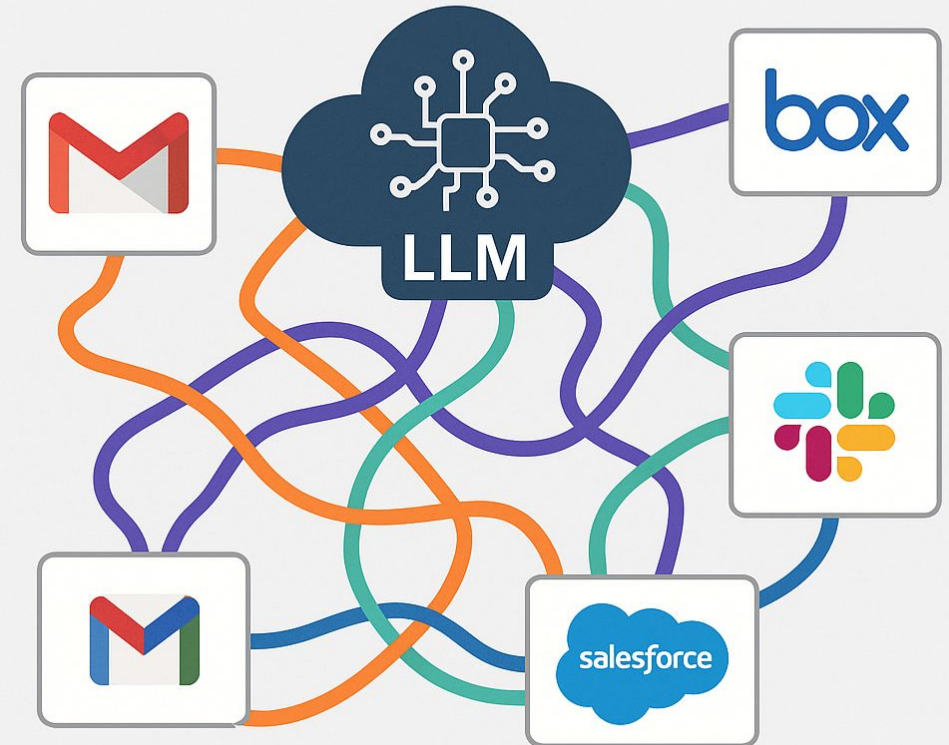
# What is MCP (Model Context Protocol)

**A new open standard from Anthropic** that allows Large Language Models (LLMs) to securely connect directly to business apps (like Gmail, Box, Slack, Salesforce)

Before MCP:

- Connecting LLMs to business apps required **custom-built integrations** or **middleware workarounds**
- Every app added meant another **fragile, one-off pipeline** to build, test and maintain

Before MCP: Custom, brittle, one-off connections



# Why MCP is a Big Deal

LLMs (like ChatGPT or Claude) have **knowledge cutoffs** - they don't know anything created after their last training date

Even worse, they **can't access your proprietary data**, like internal docs, emails, CRM records or calendars.

Out of the box, LLMs can:

- ✓ Write emails
- ✓ Answer general questions

But they **cannot**:

- 🔍 Search your inbox
- 📅 Update your calendar
- 🧩 Connect to live business systems (eg: Salesforce)

## Why MCP is a Big Deal

LLMs can't access your proprietary data

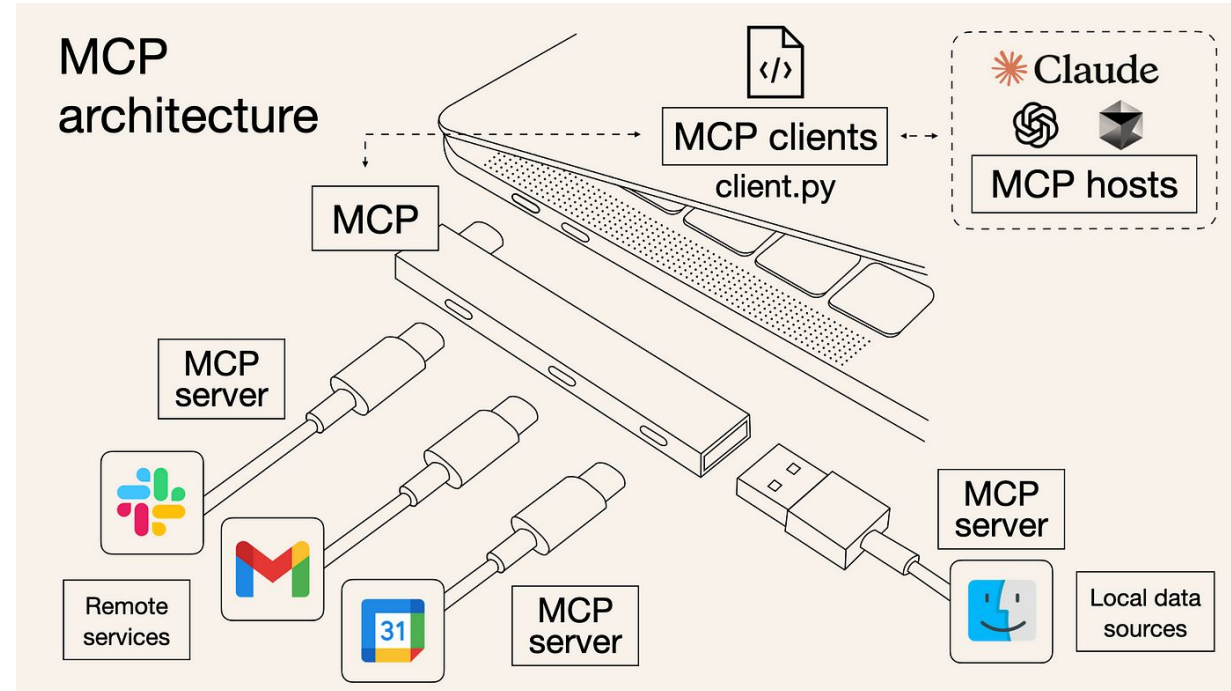


# How MCP Solves This

MCP replaces complex, one-off integrations with a **shared, open standard** for connecting LLMs to your tools

It eliminates custom code and introduces a true **plug-and-play architecture** for AI-driven workflows

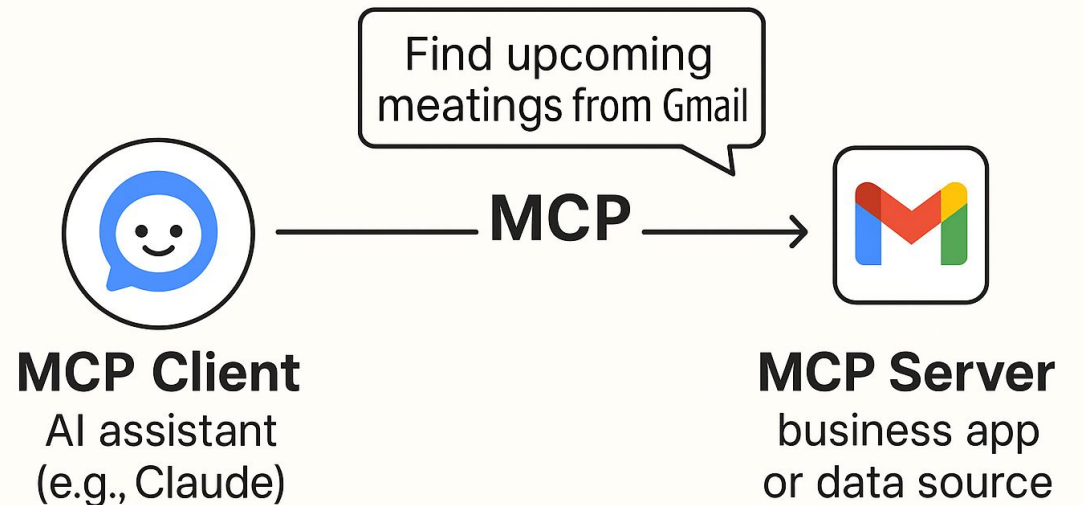
AI is no longer a siloed chat window - it's a connected system that can search, act and respond across your business apps, in real time.



# How MCP Works - Simplified

- **MCP Client** → This is your **AI Assistant** (e.g. Claude)
- **MCP Server** → The **business app or data source** you're connecting to (ie: Gmail, Salesforce)
- **MCP Protocol** → The **standard “language”** they use to talk to each other

## How MCP Works — Simplified













# Getting Started: Types of MCP Servers

MCP comes in a variety of “flavors” depending on your needs and comfort level:

- **Built-in integrations**  
(no setup required)
- **Official servers** from tool providers (e.g., Atlassian, Notion)
- **Community-built servers**  
(open source, flexible may require review)\*
- **Custom servers**  
you develop for your own use case

Type	Setup Effort	Customizability
Built-in		
Official Provider		
Community-Built		
Custom		

\*Great for developers or AI enthusiasts, but check GitHub stars and README quality

# Getting Started: Resources

There is no single authoritative source for MCP Servers

- There is talk that this is being organized.

Several sites aggregate the most popular:

- <https://mcp.so/>
- <https://github.com/modelcontextprotocol/servers>
- <https://glama.ai/mcp/servers>



# MCP Servers: Risks to be aware of

An MCP server is essentially code that runs locally with your permissions

⚠️ If poorly written or malicious, it can compromise your security or data

⚠️ Some 3rd-party servers can be **updated silently** after installation

## Rule of thumb:

Treat MCP servers just like any **third-party app**:

Only install from trusted sources and review the code or community reputation

### ✅ Safe Practice

Install from GitHub with stars

Read README and code

Use verified providers

### ❌ Risky Practice

Install random forks

Skip setup scripts

Use unmaintained servers

# MCP Servers: Recommendations

✓ **Use official MCP servers**  
published by trusted app vendors

✓ **Only install community servers with strong ratings and clear documentation**

⚠ **If you're connecting to Salesforce, use a Dev Sandbox only** - never connect production environments until fully validated



Choose MCP servers like you choose browser extensions: wisely

# Chris' MCP Recommendations

## Salesforce Community Servers:

- [Tapas Mukherjee's MCP](#)
- [Rupert Barrow's MCP](#)

## Helpful Utilities

- [Sequential Thinking](#)
- [Memory](#)
- [Perplexity MCP](#)

# Demo: Installing a Community Salesforce MCP (Claude Desktop)

## Prerequisites:

1. Create a Claude account
2. Download Claude Desktop app.
3. Download and install Node.Js

## Instructions

1. Open CMD Prompt and run this command:

```
npm install -g @tsmztech/mcp-server-salesforce
```

2. File → Settings → Developer → Edit Config

Paste:

```
{
  "mcpServers": {
    "salesforce": {
      "command": "npx",
      "args": ["-y", "@tsmztech/mcp-server-salesforce"],
      "env": {
        "SALESFORCE_CONNECTION_TYPE": "User Password",
        "SALESFORCE_USERNAME": "your_username",
        "SALESFORCE_PASSWORD": "your_password yoursecuritytoken",
        "SALESFORCE_INSTANCE_URL": "https://test.salesforce.com"
      }
    }
  }
}
```

# How to Use Salesforce MCP

AI isn't aware it has these new super powers.

Instruct it on which tool(s) to run

Examples:

- "Use `salesforce_describe_object` for the Opportunity object"
- Use `salesforce_read_apex` for <insert Apex class name>

# MCP and What It Means for Salesforce DevOps

- DevOps & AI
  - Well integrated into coding workflows
    - Native AI tools like Cursor work well with Salesforce metadata
    - Advanced prompts generate miracles
  - GenAI Applications
    - Code completion
    - Documentation Generation
      - Dynamic or Checked and Stored?
    - Root Cause Analysis
    - Infrastructure as Code generation
  - Agentic Applications
    - GitHub PR generation and management
    - Pipeline Automation
    - Incident Management
- **MCP Key Enabler → Gives Agents Actions**



# Recent Salesforce MCP Announcements

Project / Tool	Description	Status / Use Case
<a href="#">Salesforce DX MCP Server</a>	Handles code deployment, scratch org creation, and test execution through conversational interfaces.	In Developer Preview.
<a href="#">Heroku Platform MCP Server</a>	Extends MCP capabilities to the broader Salesforce ecosystem, specifically for custom server deployment on Heroku.	Official server enabling natural language commands for project management and testing on Heroku.
<a href="#">MuleSoft MCP Server</a>	Focuses on enabling API-to-MCP transformation, connecting AI agents to various backend systems via MuleSoft's integration capabilities.	Officially supported server for extending agentic workflows to enterprise systems.

# Open-Source Salesforce MCP Servers

Project / Tool	Description	Status / Use Case
<a href="#">MCP-Salesforce (smn2gnt)</a>	A Salesforce MCP connector that enables AI agents to run SOQL, SOSL, and perform metadata-aware CRUD operations. Built-in support for Tooling API and Apex REST integration.	✅ Active as of May 23, 2025. Used for secure, real-time querying and configuration of Salesforce data and metadata via AI assistants.
<a href="#">mcp-server-salesforce (tsmztech)</a>	Claude-native Salesforce MCP server. Provides fine-grained access to objects, fields, records, and Apex logic. Supports natural language instructions translated into SOQL/SOSL/Apex operations.	✅ Active as of June 12, 2025. Ideal for LLM-to-Salesforce use cases, including DevOps automation, metadata inspection, and change planning.
<a href="#">salesforce-mcp-server (kablewy)</a>	A lightweight MCP server built using jsforce to expose core Salesforce REST functionality. Includes secure OAuth flows and direct SOQL capabilities.	✅ Active as of June 5, 2025. Useful for AI-backed automation agents interacting with Salesforce records and schema metadata.

# MCP Changes Training Needs

MCP Enabled Agents are Not a Magic Pill

You Need To Know The Types of MCPs

MCP Authentication



# MCP Changes Training Needs

Deeper Knowledge of Risks Needed

Setup Knowledge

Future Automation in Mind

