Agentic AI Experience for Cisco Security Developers

Pritom Gogoi
Software Engineering Technical Leader

Kalyana Sundharam Karunanidhi
Software Engineering Architect

BRKDEV-1187

Webex App

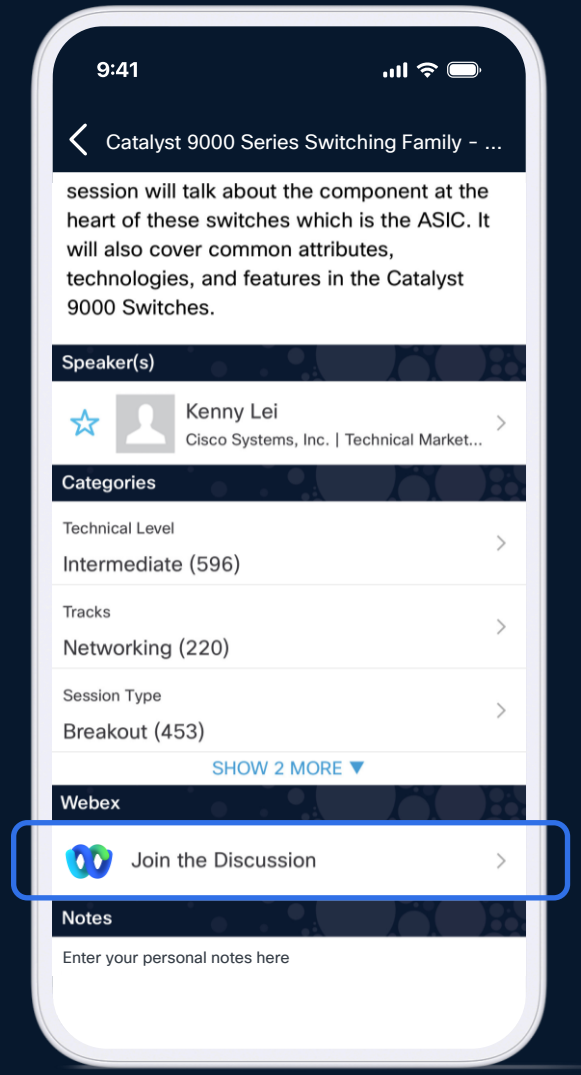
Questions?

Use Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Events App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 27, 2026.



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Speaker Bio: Kalyana Sundharam Karunanidhi

- I live near Los Angeles, United States with my wife & 2 daughters.
- With Cisco since May 2015.
- Lead Architect - Security Cloud Control.
- Started my career as a Software Engineer in 2004.
- Building cloud-native platform solutions.
- I enjoy traveling long drives with my family.
- Love to play Badminton, Chess & Hockey. Still playing US Senior Badminton open tournaments.



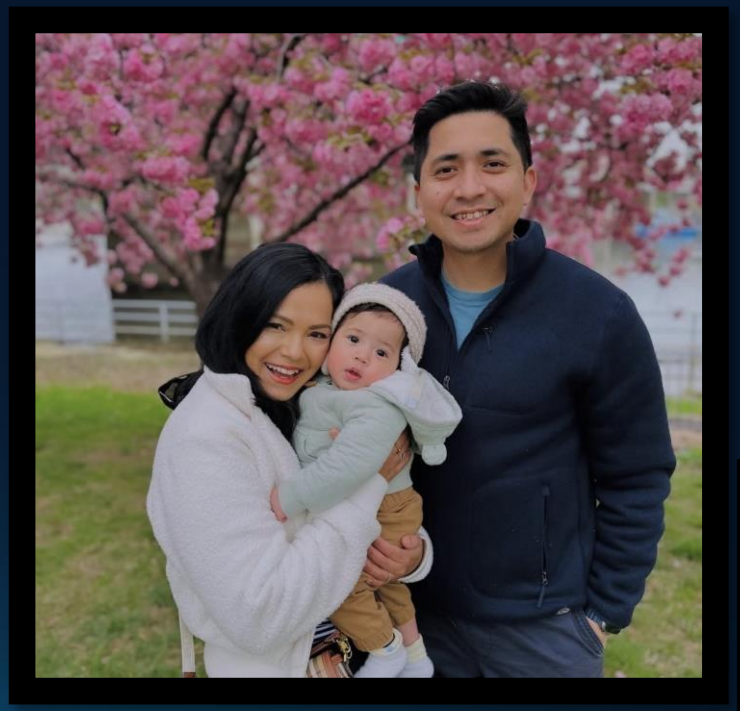


© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Speaker Bio: Pritom Gogoi

- I live in San Francisco Bay Area, United States with my wife and son
- Technical Leader at Cisco
- With Cisco since August 2018
- Passionate about building cloud-native platforms and distributed systems
- Architecting agentic platforms for developers.
- Loves going on long bike rides and exploring new trails.





© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Session Expectations

What we'll cover and what we won't

Agenda

1. The Developer Integration Landscape - Today
2. Agentic AI – The Paradigm shift
3. The Missing Contract - Introducing MCP
4. Agentic Experience in Action (Live Demo)
5. Key Takeaways

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

The Developer Integration Landscape – Today

Where we are: Direct APIs, scripts, SDKs

How Developers Integrate APIs today

1. Direct API calls
2. SDKs and client libraries
3. Custom scripts and glue code
4. Workflow orchestration

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Common Integration Patterns

1. Pagination loops (pages, cursor)
2. Error handling and retires
3. ID chaining across API calls
   (e.g get_org -> get_orgId -> get_users)

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Developer's Pain Points

1. Large amount of boilerplate code
2. Fragile, multistep workflows
3. Small API changes break integrations

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Agentic AI: The Paradigm Shift

From scripts to agents – what changes and why it matters

CISCO Live !

Agentic AI

A system where you provide a goal,
not step-by step instructions

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

The Paradigm shift

Imperative

1. "Call API A, then B and C"
2. Developers manage control flow

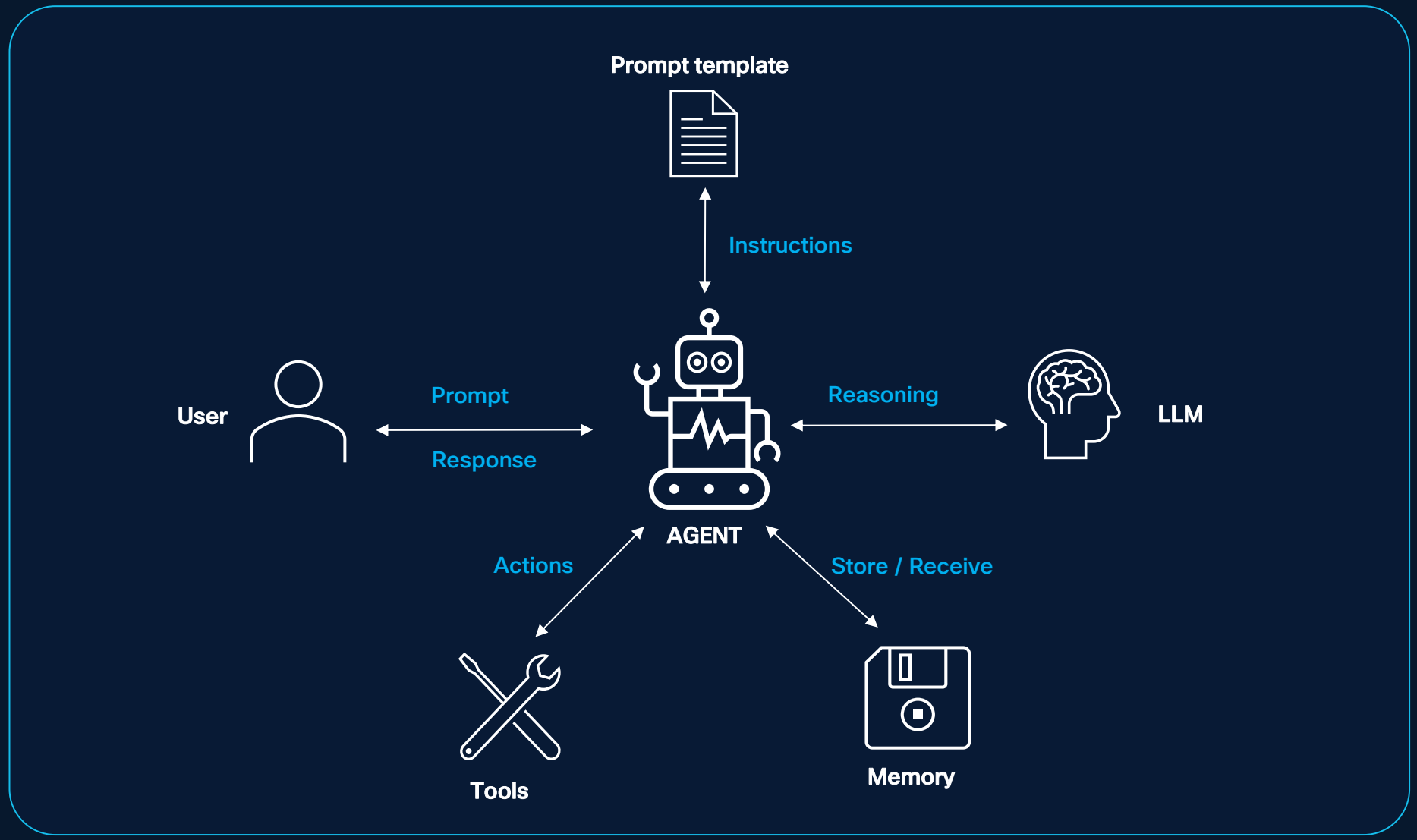
Declarative

1. "Get all users in my organization"
2. Agent determines how to achieve the outcome

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Agent - Building Blocks



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

APIs were designed for humans, not LLMs

1. Deterministic Caller
2. Explicit Intent
3. Human Judgement
4. Documentation driven workflows

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

The Missing Contract: Introducing MCP

Introduction to MCP (Model Context Protocol)

1. A standard protocol for exposing capabilities to agents
2. Defines how tools are
   - Described
   - Discovered
   - Invoked
3. Separates reasoning from execution

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

What MCP guarantees

1. Standard, interoperable tool contract
2. Explicit, deterministic tool invocation
3. Clear control & security workflows
4. Framework & language agnostic

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

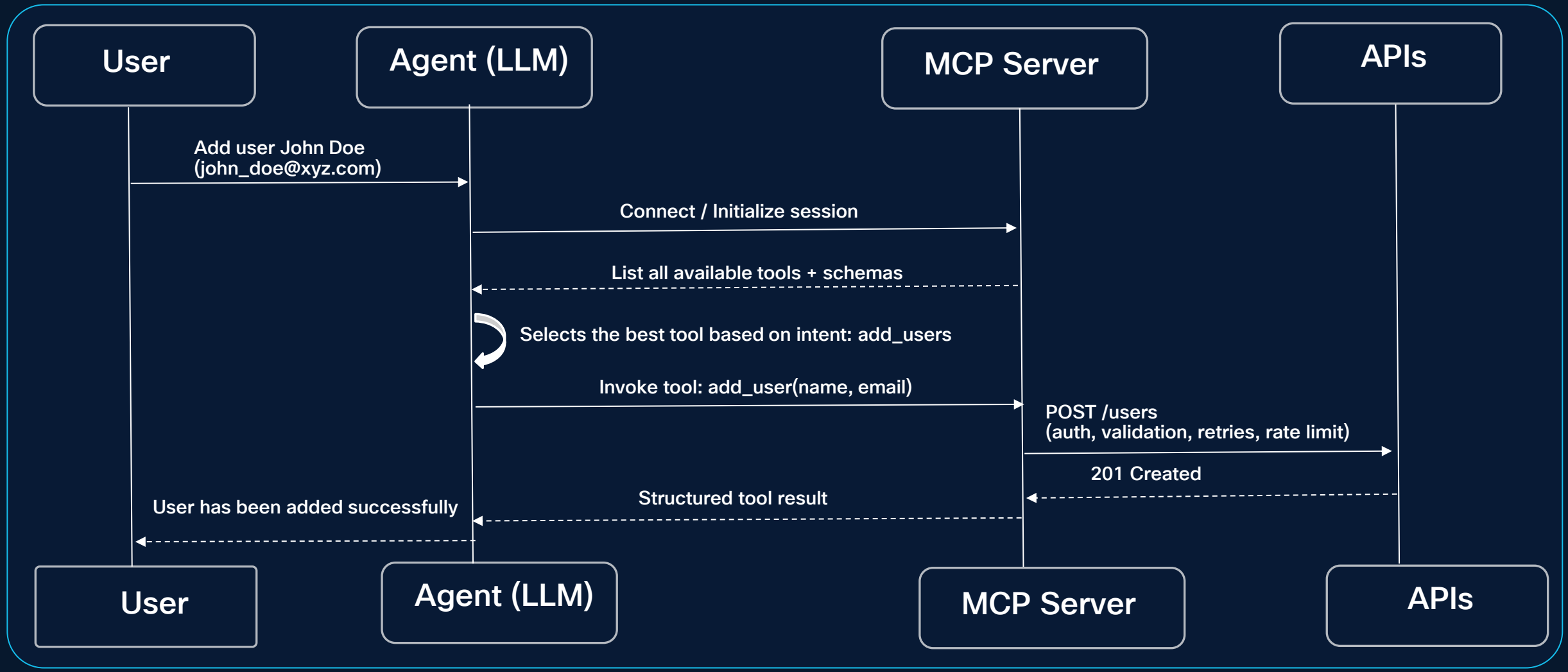
What MCP DOES NOT do

1. NO autonomy
2. NO reasoning
3. NO hallucinations prevention
4. NO security out of box

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

How Agents Discover and Invoke Tools



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

How MCP solves API limitations for Agents

Scenario – Get all users from an organization

No Contract vs Contract

Without MCP

Prompt

```
You can call the Users API to get users for an org.
Endpoint: GET /v1/orgs/{orgId}/users
Query params: status
Use Bearer token.
```

Code

```
requests.get(
    f"/v1/orgs/{orgId}/users",
    params={"status": "active"},
    headers={"Authorization": token}
)
```

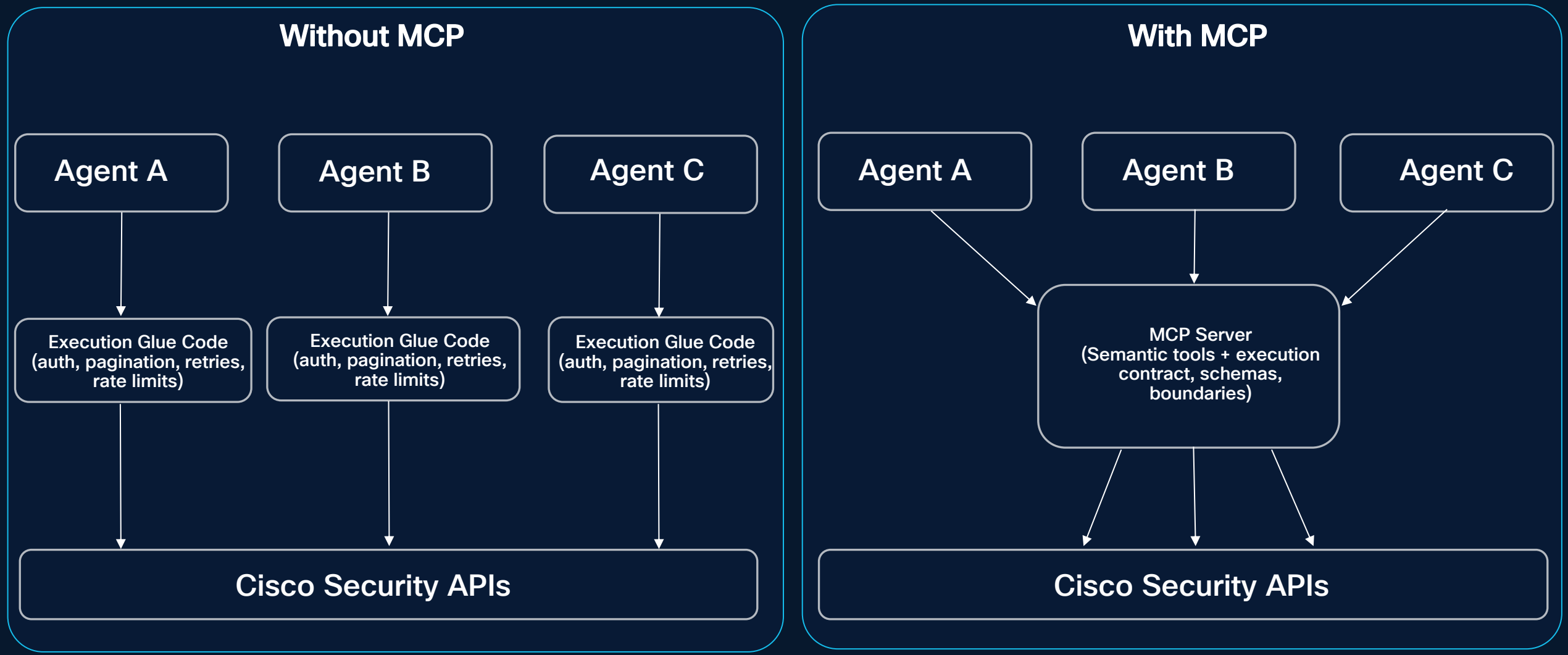
With MCP

```
"tools": [
    {
        "name": "get_users_by_org_id",
        "description": "Retrieve all users belonging to a specific organization",
        "inputSchema": {
            "type": "object",
            "properties": {
                "orgId": {
                    "type": "string",
                    "description": "Unique identifier of the organization"
                },
                "status": {
                    "type": "string",
                    "enum": [
                        "active",
                        "inactive",
                        "all"
                    ],
                    "description": "Optional filter for user status"
                }
            },
            "required": [
                "orgId"
            ]
        }
    }
]
```

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

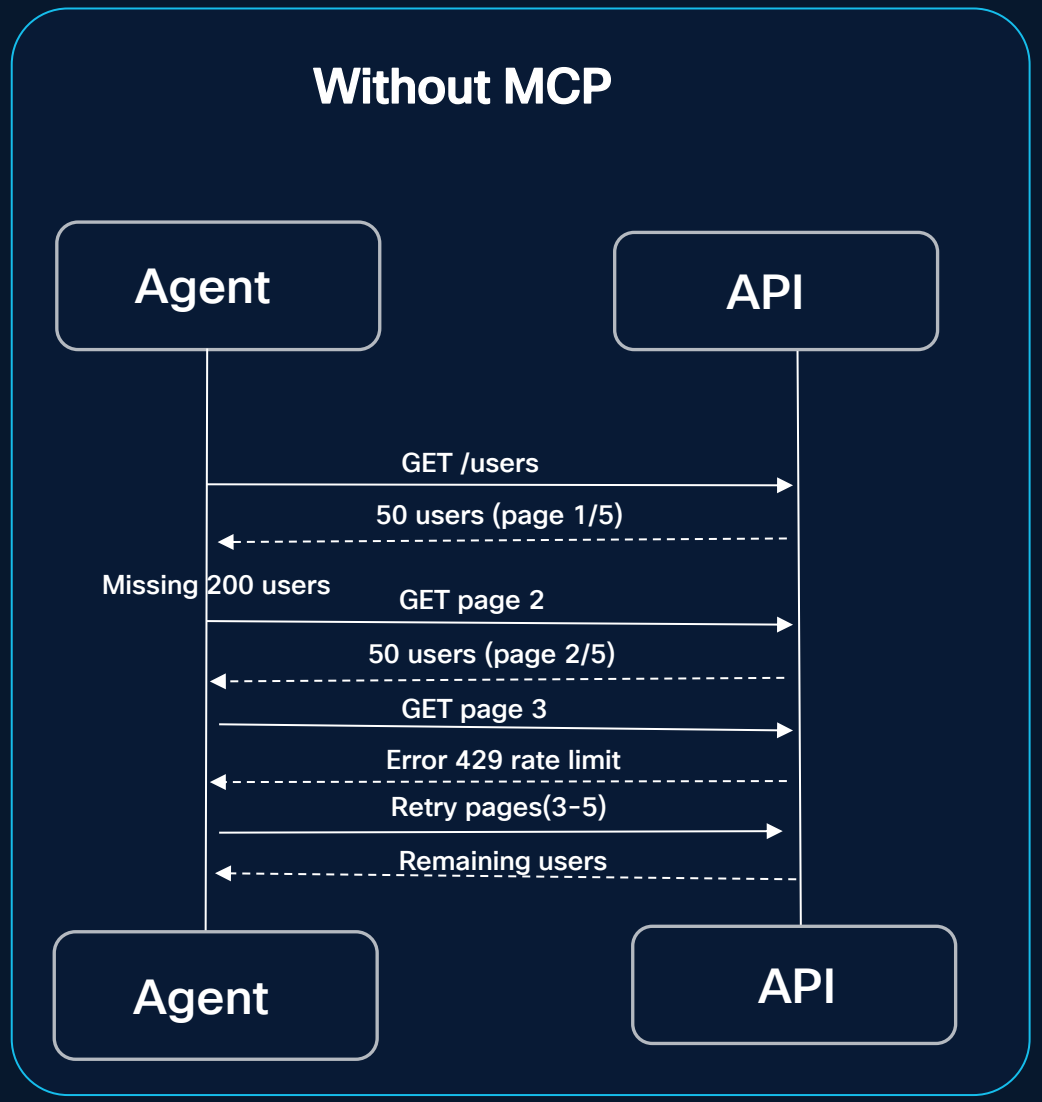
LLM’s reason, MCP executes

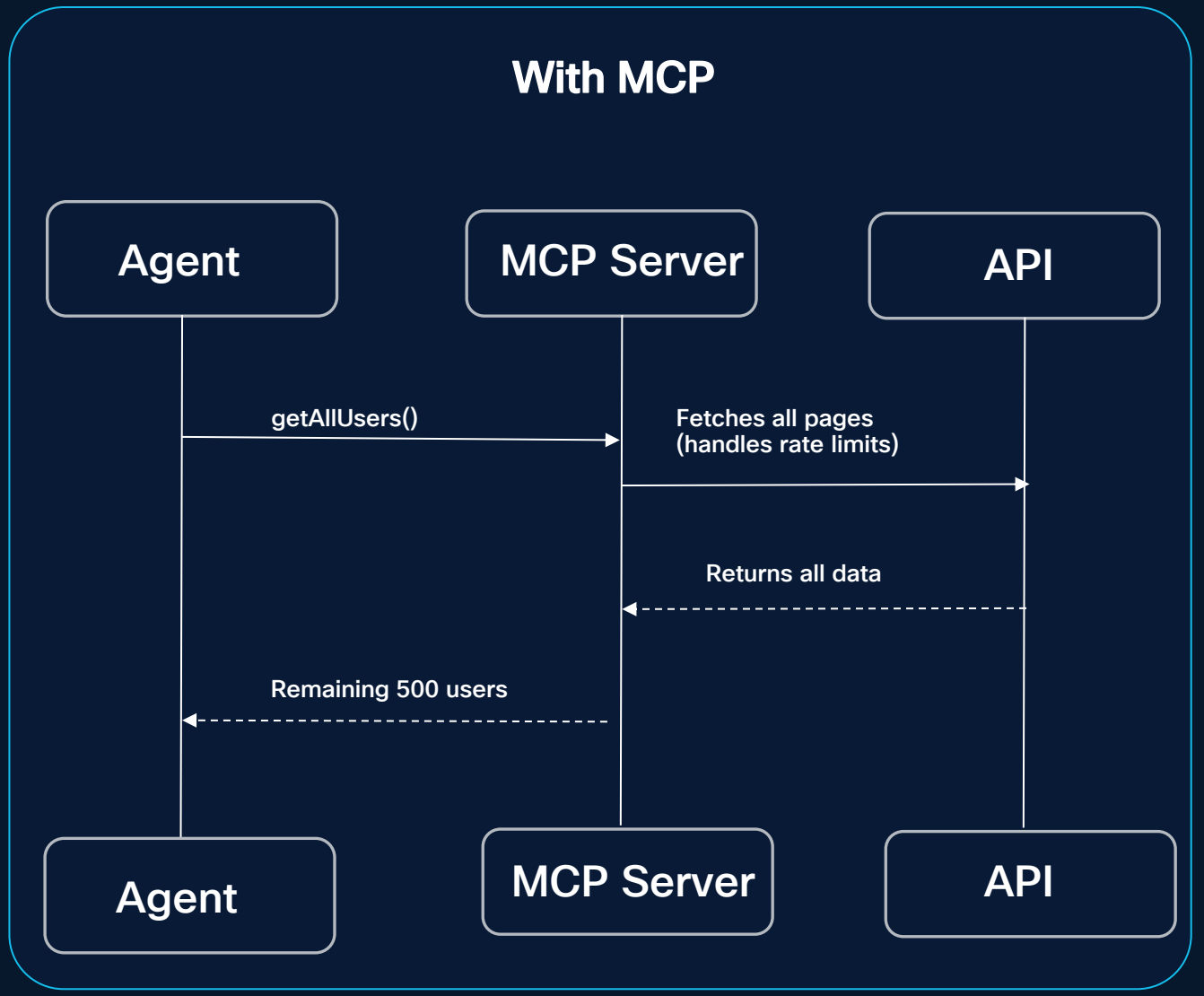


© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

API complexity absorption





© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

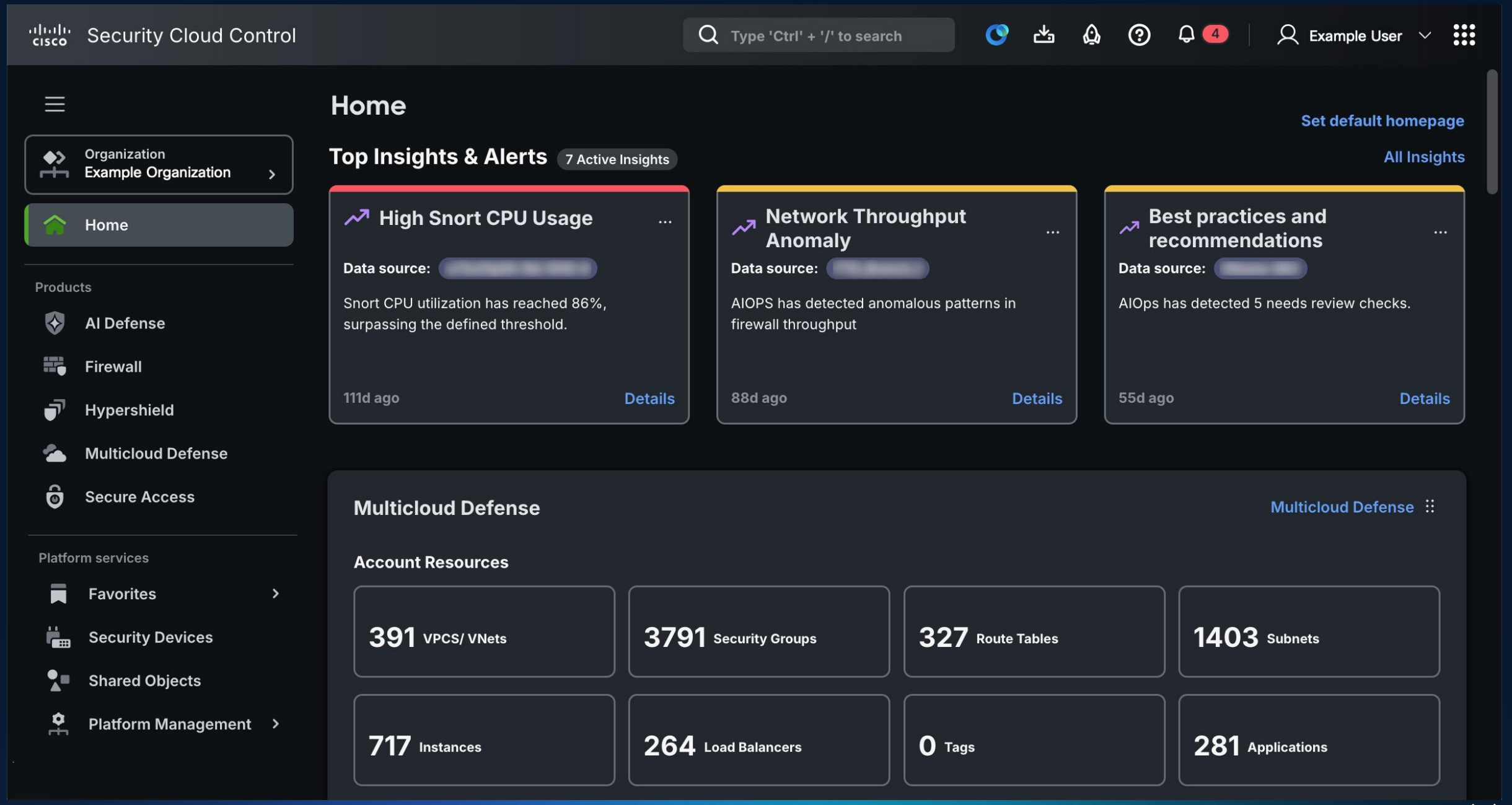
MCP as API Interpreter for LLMs

1. **Absorbs API complexity**
2. **Provides LLM-Native Interfaces**
3. **Structured Error Handling**

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Security Cloud Control



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Security Cloud Control



Product Provisioning



Security Cloud Sign-On



IAM & RBAC



Unified Dashboard & Integrated Product Dashboard



Security Developer Experience



Unified UX



Unified AI Assistant

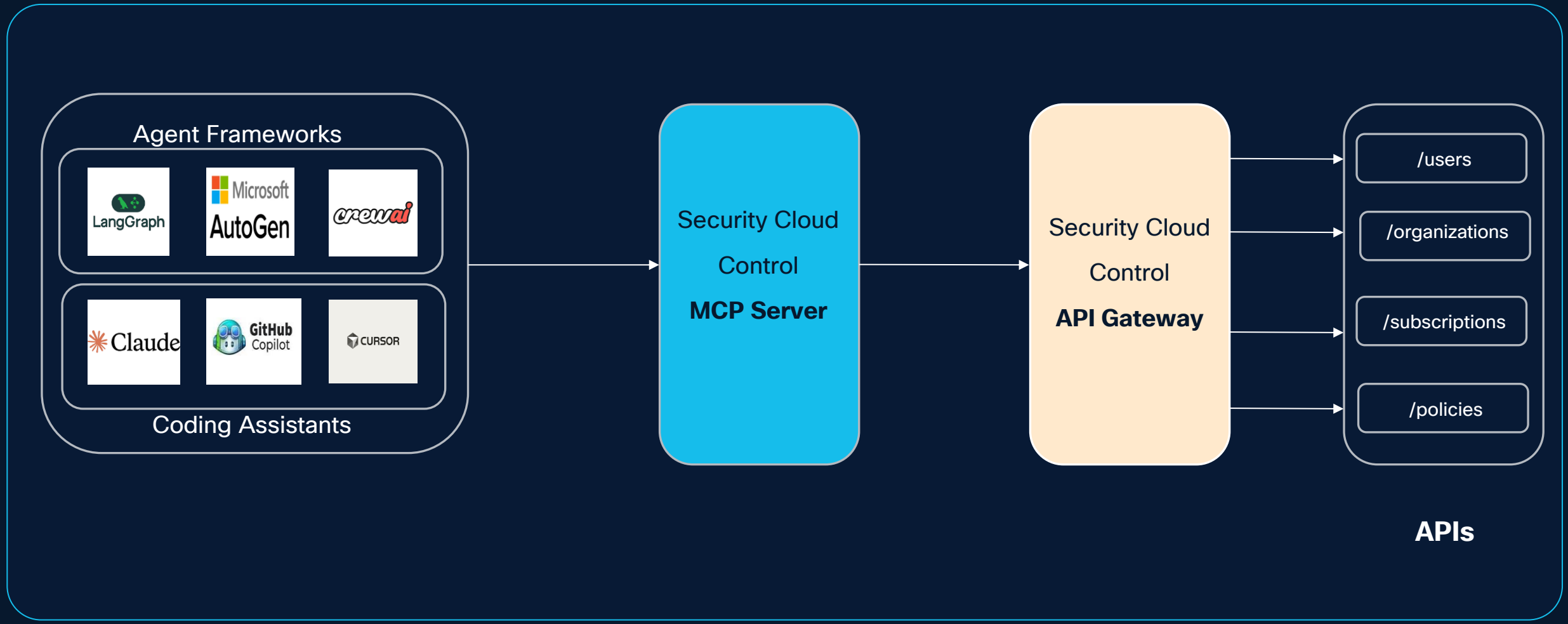


MSP & FedRAMP Support

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Security Cloud Control MCP Architecture



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Agentic Experience in Action

(LIVE DEMO)

Challenges & Mitigation

Challenges	Mitigation
Tool Explosion & Context Bloat	High Level semantic tools
Prompt Injection & Tool Poisoning	Implement input validation with semantic filtering
Confused Deputy Problem	Implement proper authentication and authorization checks

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Key Takeaways

1. The Paradigm Shift

   From Imperative "How" to Declarative "What"

2. MCP as the Universal Translator

   Standardized Discovery, Invocation, and Context Flow

3. Security cannot be an afterthought

   Design for Least Privilege and Containment from Day One

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Complete your session surveys



Complete your surveys in the Cisco Events App.



Complete a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer meeting

Visit the Technical Solutions Clinics to discuss your technical questions



Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at CiscoLive.com/On-Demand

© 2026 Cisco and/or its affiliates. All rights reserved.

Thank you




CISCO