

Atlas MCP

Findings, vulnerabilities, assets, and tickets. Inside the AI assistant your team already uses. Asked in plain language, bound to your identity.

The Answer is in Atlas. Your Team is Somewhere Else.

More of your team's work now happens inside AI assistants: Claude, Copilot, Cursor, and Codex. The data they need to act lives in a security portal. So every question costs a context switch. Log in, filter the findings, cross-check the asset, look up the CVE, open a ticket. Attackers get that time for free.

Atlas MCP connects your AI assistant directly to Atlas. Ask about findings, vulnerabilities, assets, and tickets in plain language, and get answers from your Atlas data without leaving the tool you're in. The server is hosted, so there is nothing to install. Access is bound to each user's identity and gated by read and write permissions. It's already on for every Atlas user.

4 in 5

SOC practitioners reach for AI or machine learning tools in their daily work.

SANS Institute, 2026 SOC Survey

1 in 3

Of those teams have built AI into a defined workflow with governance and validation.

SANS Institute, 2026 SOC Survey

-7 days

Estimated mean time to exploit. Exploitation now routinely lands before the patch.

Mandiant, M-Trends 2026

What Atlas MCP Delivers

Ask in Plain Language

- ✓ *Findings*: list them, pull details and full signal data, and update them
- ✓ *Vulnerabilities*: list CVEs and get the details on each
- ✓ *Assets and patches*: list assets, get details, and see missing patches
- ✓ *Tickets*: list, read, comment on, create, and update support tickets

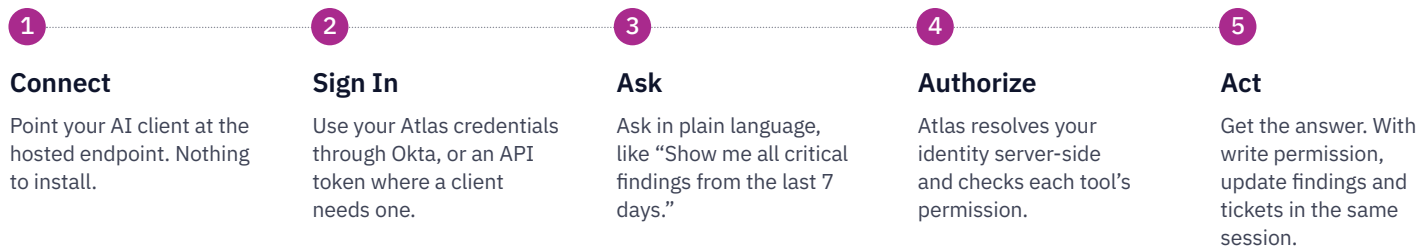
Works Where You Work

- ✓ Claude on the web, desktop, and Claude Code, through OAuth
- ✓ VS Code with GitHub Copilot, through OAuth with a token fallback
- ✓ GitHub Copilot CLI, Cursor, and Codex, through an API token
- ✓ Any client that supports remote MCP over Streamable HTTP with custom headers

Access You Control

- ✓ Okta sign-in binds access to your identity, with no secret stored on the client
- ✓ Identity resolved server-side, where the client can't set it
- ✓ Every tool gated on read or write permission, so a read-only token can't create or update anything
- ✓ On by default, with a per-user off switch for administrators

How It Works

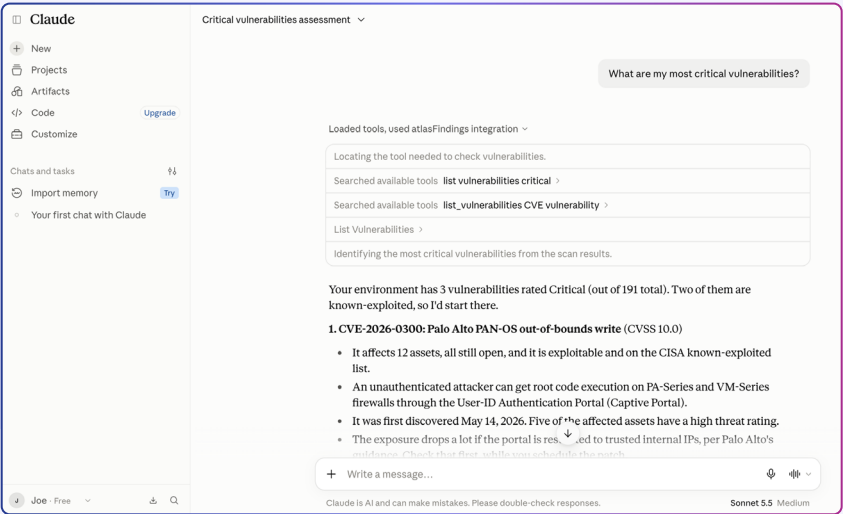


See Atlas MCP in Action

TRY ASKING:

- ▶ “Show me all critical findings from the last 7 days”
- ▶ “List assets with critical vulnerabilities”
- ▶ “Show me my open support tickets”

A typical findings query returns in under a second.



Where Atlas MCP Works

CLIENT	SIGN-IN	GOOD TO KNOW
Claude (web, desktop, Claude Code)	OAuth	Fastest path is the Claude directory. Connect, sign in, and tools appear in seconds.
VS Code with GitHub Copilot	OAuth, token fallback	Copilot Chat must be in Agent mode for Atlas tools to be callable.
GitHub Copilot CLI	API token	Add it with /mcp add, or directly in ~/.copilot/mcp-config.json.
Cursor, Codex, and other clients	API token	Any client with remote MCP over Streamable HTTP and custom headers.
Microsoft 365 Copilot	Admin-led connector	Federated connectors are read-only. Your TAM supplies the connector metadata.
Chat GPT	In progress	Not available yet. OAuth support is in progress, and your TAM can flag you for it.

15
Tools; 12 read-only and 3 write

5+
AI clients by name, plus any streamable HTTP client

0
Local installs, because the server is hosted

<1s
For a typical findings query

Outcomes You Can Expect

- ✓ Answers from Atlas without leaving the IDE, terminal, or assistant your team already uses
 - ✓ Triage in one thread, with findings, signal data, assets, and CVEs pulled together as you ask
 - ✓ Support tickets created, updated, and commented on in the same session, with write permission
- ✓ Every request tied to a named Atlas identity, with read and write enforced server-side
 - ✓ Administrators in control, with a per-user off switch
 - ✓ Partner Super Admins navigating child accounts and scoping a query to one child organization

“We look at eSentire to be the experts. We trust them implicitly. They’re with us through the thick and thin till the end.”

CISO, Financial Services [GARTNER PEER INSIGHTS](#)

2,000+ organizations in 80+ countries | 25 years of SOC expertise | 2M+ endpoints protected | MDR Leader, IDC Marketscape for MDR



Assume the attacker is already moving.

Ask Atlas what changed, and what to do about it.

SPECIFICATIONS	
Endpoint	https://api.esentire.com/mcp/rpc
Transport	Remote MCP over Streamable HTTP, hosted by eSentire. No local process, no proxy, no npx.
Authentication	OAuth through Okta, recommended. API token fallback, issued read-only or read-write at atlas.esentire.com/settings/auth.
Authorization	Identity resolved server-side from the credential. Every tool gated on read or write permission.
Tools	15 tools, 12 read-only and 3 write, across Findings, Tickets, Assets, Vulnerabilities, Patches, and Signals.
Admin Control	On by default for every Atlas user. Switch it off per user in Settings → User Management → Application Access.
Partner Mode	Partner organizations with the Super Admin role get organization-tree tools to navigate child accounts and scope a query to one child.

Get Connected



CLAUDE

Go to claude.ai/directory/atlasfindings, select Connect, and sign in with your Atlas credentials. Tools appear within seconds.



EVERY OTHER CLIENT

Point it at <https://api.esentire.com/mcp/rpc>, and follow the Atlas MCP Setup Guide for your client.



QUESTIONS

Your **Technical Account Manager** can supply Microsoft 365 connector metadata and flag you for ChatGPT support when it lands.

LET’S TALK SECURITY →

IF YOU’RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US 📞 1-866-579-2200

eSENTIRE

eSentire is a leader in Controlled Autonomy SecOps, protecting 2,000+ organizations across 35+ industries around the world. Founded in 2001, the company’s Controlled Autonomy SecOps operating model pairs agentic AI operatives with engineered human-judgment controls, delivering expert-depth security outcomes at machine speed without ceding accountability to opaque automation. Powered by the unified agentic AI Atlas Platform, eSentire’s Atlas AI + 24/7 expert human SOC coverage delivers offensive capabilities that preempt exposures before attackers do, detect, and respond to stop threats in real time. For more information, visit www.esentire.com and follow @eSentire.