crawdad.

Reseller Partner Brief

Agent security you can bring to your clients

FOR MSSPs · SECURITY & AI CONSULTANCIES · SOLUTION PARTNERS

ANDREW SISPOIDIS · FOUNDER · GETCRAWDAD.DEV · 2026

Add agent security to what you already deliver.

A partnership for firms whose clients are putting AI agents into real use.

Andrew Sispoidis, Founder · getcrawdad.dev · andrew@getcrawdad.dev

What Crawdad is

Crawdad is a runtime security layer for AI agents. It runs locally, as a transparent proxy between a client's agents and the model providers they call. Every request passes through a detection pipeline that catches **prompt injection, credential leakage, and data exfiltration** in real time, and a policy engine decides what the agent is allowed to do. It installs with one command, needs no code changes, and works with any agent framework and any model. Detection runs on the client's own machine, so their data never leaves by default.

The problem it solves for your clients

AI agents now act with real credentials and real permissions. They read inboxes, query databases, call tools, and move data. But a model cannot reliably tell instructions from content, so a hidden instruction in a web page, a document, or a tool response can hijack an agent into acting against its owner, with full authorization and **no alert and no way to know.** The existing stack, firewalls, EDR, DLP, identity, does not understand agent behavior. This is the gap.

Why now

Your clients are deploying agents this year, not next. The security teams know the old controls do not cover them, and they are looking for an answer before an incident or an audit forces one. Bringing that answer is a reason to be in the room, and a new line of recurring work.

> WHAT'S VERIFIABLE TODAY
>
> **99.8% detection** on a public, reproducible benchmark · **local-first** by architecture · independently validated through the **Anthropic Cyber Verification Program** · built in Rust, 607 tests, in production.

Why it belongs in your practice

Protect your clients

Real enforcement that blocks attacks, not another dashboard of alerts.

Win the clients others can't

Local-first and zero-egress by architecture, the only fit for regulated and air-gapped buyers who cannot use a cloud scanner.

A recurring line

Margin on every client you bring and keep, with simple delivery and no code changes.

Who we're looking for

Firms whose clients are deploying AI agents and who are trusted to secure them: managed security providers, security and AI consultancies, systems integrators, and vCISO practices. The fit is strongest where your clients are in regulated or sensitive environments, because that is where Crawdad is not just better but the only architecture that fits.

How the partnership works

REFER — **You introduce, we close and support**

A recurring referral share on the revenue from clients you bring. The lightest way to start.

RESELL — **You sell and own the relationship**

You carry Crawdad in your offering at partner margin, with our enablement behind you. Recurring margin for as long as the client stays.

EMBED — **You bundle it into your managed service**

Crawdad becomes part of what you deliver and operate, at wholesale terms. Local-first means it deploys cleanly inside client environments, including air-gapped ones.

Deals you register are protected, and exact economics are set with each partner. We keep it simple.

How to start

1

A short call to find the fit and the model that suits your practice.

2

A scoped evaluation, so you see exactly what it does in your world.

3

First client, then we build from there together.

Andrew Sispoidis · Founder · andrew@getcrawdad.dev