Straiker

PORTFOLIO BRIEF

AI is the biggest technology shift of our lifetime, and agentic AI adoption is exploding but so are the risks. Agents are reading your email, managing your calendar, writing your code, and building more agents. They inherit your permissions and act with the authority of the people who deployed them. A compromised agent doesn't need to break in. It's already inside.

Traditional security tools don't understand agents. They weren't built for MCP servers, tool chaining, memory, skills, indirect prompt injection or autonomous multi-step actions. Straiker is.

THE STRAIKER DIFFERENCE

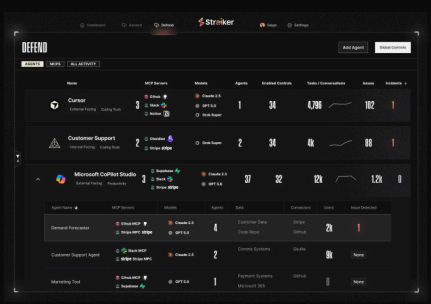
Purpose-built for agents. Works with the stack you already have.

DISCOVER AI

VISIBILITY & GOVERNANCE FOR AGENTS

FRICTIONLESS DISCOVERY

- See every agent, model, and internal and external MCP server
- Identify what data each agent accesses and who controls its instructions
- Block risky MCP integrations using a database of 12,000+ scanned MCP servers
- Enforce governance policies across every agent you buy or build
- Frictionless for developers with visibility across multi-cloud and every framework

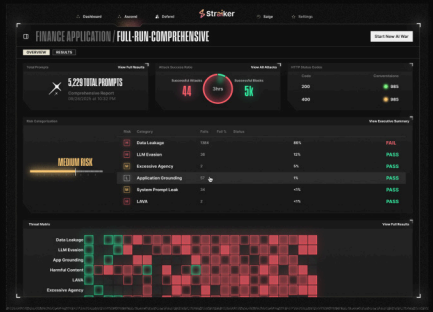


ASCEND AI

CONTINUOUS ADVERSARIAL AGENT TESTING

HIGHEST ATTACK SUCCESS RATE IN THE INDUSTRY

- Probe agents for prompt injection, manipulation, and data exposure across every lifecycle stage
- Tests the full attack surface: RAG pipelines, tool chains, MCP servers, and customer-facing interfaces
- Run assessments on-demand, scheduled, or always-on, tailored to your goals and risk tolerance
- Compliance assurance across HIPAA, EU AI Act, PCI DSS v4.0, NIST 600-1, and OWASP

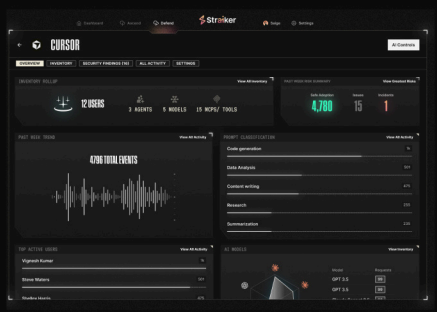


DEFEND AI

RUNTIME SECURITY FOR AGENTS

98+% ACCURACY, <400 MS LATENCY

- Detects and blocks prompt injection, LLM evasion, data leakage, tool misuse, and MCP exploits across every agent type
- Full agentic trace: know exactly what your agents read, did, and said
- 98%+ accuracy at under 300ms, faster than frontier models
- Multimodal detection across text, code, PDFs, images, and audio
- Inline or out-of-band across any cloud, framework, or architecture



THE SECURITY CHALLENGE WITH AI AGENTS

CODING AGENTS

Developers once reviewed every line of code. Now agents write it, execute it, and commit it. They inherit credentials, but are nearly impossible to observe — making it easy to pull in packages no one vetted, connect to MCP servers no one approved, and spawn more agents that are invisible to your security team.

PRODUCTIVITY AGENTS

Productivity agents read your email, access your calendar, and act across your entire SaaS stack. Indirect prompt injections in emails or docs can hijack everything a productivity agent does next. When data leaves, it leaves silently — no malware, no alert, no audit trail.

CUSTOM BUILT AGENTS

Custom-built agents carry the highest blast radius of any agent type. They run with elevated trust, connect to your most sensitive systems, and are deployed across cloud environments with no unified security layer. A poisoned MCP server or tainted RAG pipeline can silently corrupt everything they do.

STRAIKER SECURES EVERY AI AGENT YOU BUILD OR BUY

STRAIKER'S KEY BENEFITS

GAIN FULL VISIBILITY INTO EVERY AI AGENT AND MCP CONNECTION

FIND AND FIX EXPLOITS BEFORE ATTACKERS CAN USE THEM

DETECT AND STOP THREATS TARGETING YOUR USERS AND AI AGENTS

GreenLIGHT · American Express Global Business Travel · FITNESS · COMCAST · DIRECTV · Automation Anywhere

Straiker is the agent security company. Powered by a proprietary AI engine trained by the Straiker STAR Labs Research Team, Straiker enables enterprises to discover their AI agent footprint, continuously test agents through adversarial methods, and defend against threats at runtime with 98%+ accuracy and sub-second latency. Learn more at straiker.ai

Get a Demo | **Assess Your Agent**

© 2026 Straiker | 650-651-8338 | info@straiker.ai