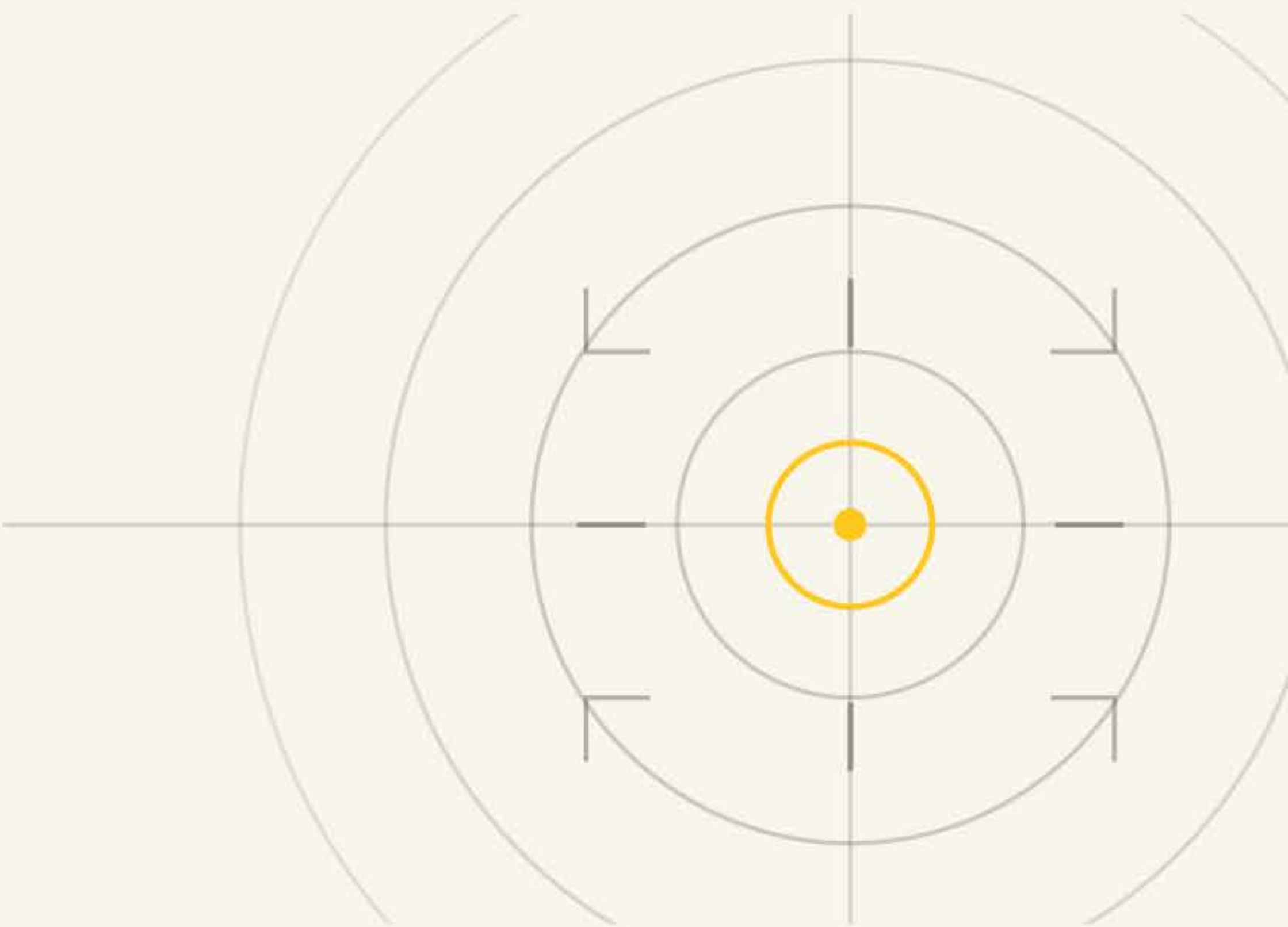


STRAIKER STAR LABS • THE AGENTIC THREAT MODEL

YOUR AGENTS AREN'T IN DANGER. THEY ARE THE DANGER.



SILENT UNAUTHORIZED ACTION

85%

of successful attacks caused an agent to **silently do something it was never authorized to do**.

CODING AGENTS → RCE

36%

of successful attacks on **coding agents** resulted in remote code execution.

PRODUCTIVITY → EXFILTRATION

91%

of successful attacks on **productivity and consumer agents** resulted in silent data exfiltration.

SOURCE STRAIKER STAR LABS • DOZENS OF CYBER AGENT EVALUATION CAMPAIGNS • SOURCE STRAIKER STAR LABS • DOZENS OF CYBER AGE

THE STRAIKER DIFFERENCE



DISCOVER AI01

Frictionless discovery for visibility and governance across your agentic estate.

- ✓ Meet your environment where it is — endpoints, APIs, gateways, SaaS.
- ✓ Map agents to the models, tools, MCPs, skills, data and permissions they reach.
- ✓ Surface risky permissions, unsanctioned connections, malicious components.
- ✓ Block or revoke risky MCP and tool access.



ASCEND AI02

Autonomous adversarial testing with the highest attack success rate in the industry.

- ✓ Deploy an agentic red teamer built to attack AI agents and applications.
- ✓ Probe, adapt and chain attacks across prompts, tools, MCPs, skills, memory.
- ✓ Keep attacking until it succeeds or hits the limits of the assessment.
- ✓ Uncover real impact — RCE, exfiltration, tool abuse, unauthorized actions.



DEFEND AI03

Stop agentic threats with 98%+ accuracy, from malicious actions to rogue agents.

- ✓ Detect what the agent actually does — RCE, file access violations, exfiltration.
- ✓ Write your own policies; configure controls to Detect or Protect.
- ✓ Enforce on the full agentic trace plus user, tool, network and data context.
- ✓ Protect across models, frameworks, clouds, gateways and architectures.



AI AGENT KILL SWITCH

TAKE IT OFFLINE IN SECONDS.

Take control of a rogue or compromised agent. Stop one agent — or your entire agentic estate.



CUT OFF TOOL ACCESS



SUSPEND THE SESSION



TAKE THE AGENT OFFLINE



STOP ONE OR MANY AGENTS



ISOLATE THE AGENT



PRESERVE THE EVIDENCE

STRAIKER AI AGENT KILL SWITCH • STRAIKER AI AGENT KILL SWITCH • STRAIKER AI AGENT KILL SWITCH • STRAIKER AI AGENT KILL SWITCH

STRAIKER AGENTIC SECURITY STRAIKER.AI 01 / 02

THE STRAIKER CONTROL PLANE

AGENTIC SECURITY CONTROL PLANE

Secure every agent you build.
Secure every agent your workforce is using.

EVERY AGENT IN THE ESTATE

