FOR ENTERPRISE & MSSP

Real adversarial testing for modern agentic AI — not legacy config-scanning repackaged as AI security.

Your AI agents call other agents, which call tools, which call more agents. RedLens tests the whole chain — cascading privilege escalation, shadow AI your teams already adopted, and instant virtual patches — priced by workflow, not capped by asset count.

THE CHALLENGE

- Agent chains cascade privilege silently — a higher-privilege agent blindly trusting a lower-privilege agent's output lets an injected payload propagate hop-by-hop.
- Engineering and business teams adopt AI tools and agent frameworks faster than security can inventory them — "the copilot nobody filed a ticket for."
- Confirmed findings need a mitigation the same day, not whenever the permanent fix clears the normal release cycle.

HOW REDLENS HELPS

Multi-Agent Swarm Simulator

Traces injected payloads hop-by-hop across agent DAGs and maps compromised hops to the tools and data they could reach — most competitors don't test this at all.

Blast Radius Mapper

Ingest your agent's tool schema (OpenAPI, Anthropic, or OpenAI format) and see what a hijacked agent could actually reach: attack chains, permissions, an auditable score.

Dynamic Virtual Patch Generator

Every confirmed finding can generate a deployable mitigation — system-prompt wrapper, sanitizer rules, WAF-style rules, executable middleware — ship immediately.

Shadow AI Discovery

Passive detection of unmapped AI models and agentic calls in outbound traffic — the agent nobody filed a ticket for is the one that never got tested.

COMPLIANCE & DEPLOYMENT

Enterprise includes **Splunk SIEM integration (HTTP Event Collector)** — findings arrive field-parsed and searchable alongside the rest of your security telemetry.

Full air-gapped Docker deployment and automated HIPAA/NIST compliance audits are available on Enterprise for organizations that need a fully self-hosted, on-premise model.

MSSP & partner program: multi-client mode, white-label reporting, and unlimited monitored workflows across client accounts are available through RedLens's Enterprise/MSSP partnership track.

PRICING

RedLens prices around monitored production workflows and included attack simulations, not a capped asset count. Professional covers up to 25 monitored workflows; Enterprise removes the cap entirely and adds SIEM integration, air-gapped deployment, and a custom SLA.

PLAN	PRICE	WHAT'S INCLUDED
Developer	$799/mo	1 AI agent under test, self-serve, no procurement call required
Professional	**$8,000/mo**	**Up to 25 monitored production workflows, 50,000 attack simulations/mo**
Enterprise	$150k/yr+	Unlimited workflows, air-gapped Docker deployment, custom SLA available

See what a compromised agent could actually reach in your stack.

Run a free assessment: redlens.ai/poc · Book a demo: calendly.com/redlensai/30min · sales@redlens.ai