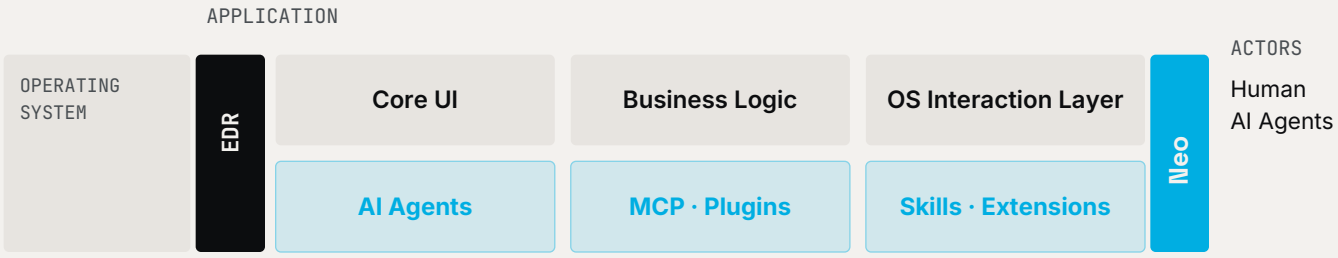
EVERY APP IS BECOMING AN AGENT

Discovery is not control.
Neo is built for both.

Agents, skills, plugins, MCP servers, browser extensions, CLIs, and applications. Neo inventories, governs, and controls every piece of software your employees run. Every endpoint, managed or unmanaged. In real time.



EDR **One interface.** The OS-to-app boundary, where system calls cross. By design.

Neo **Everything inside the application,** plus the actors driving it. Where agents, plugins, and extensions now live.

01 / WHAT CISOS TELL US — The endpoint software surface has changed faster than the controls

> *"We have no inventory of the AI agents, plugins, and MCP servers our engineers have installed. Our app control stops at signed binaries."*
>
> SPRAWL & VISIBILITY

> *"Our EDR was built for the OS layer. It cannot see an AI agent reading credentials or exfiltrating data through a sanctioned API."*
>
> DIFFERENT LAYER

> *"When something breaks, we cannot answer the only question that matters. Was that action a human, or an agent operating on a human's session?"*
>
> NO ATTRIBUTION

> *"Auditors and the board want to know how we govern AI use. Shadow-AI tools show us what is running. They cannot stop a thing."*
>
> DISCOVERY WITHOUT ACTION

02 / WHY NOW — $70B spent on endpoint, network, and identity. None of it covers this.

40%
of enterprise apps will embed AI agents by year end
GARTNER

3 in 4
boards approved major AI investments. Most have not put AI risk on the agenda.
GRANT THORNTON 2026

79%
of enterprises have agent blind spots today
AKTO RESEARCH

1 in 8
AI breaches already involve agentic systems
HIDDENLAYER 2026

AN AI-NATIVE PLATFORM FOR AN AI-NATIVE WORLD

Built agentic. Detects agentic. Operates at AI speed.

01 · PROCESS
Agentic Research
A workforce of agents continuously discovers, classifies, and assesses every piece of software in your environment. Marketplace crawlers, documentation analysis, static and runtime sandboxes.

02 · DETECTION
Agentic Detections
Detection logic adapts as the agentic threat surface evolves. Auto-policy creation. No signature updates to wait for. The platform learns the threat as fast as it appears.

03 · SPEED
AI Speed
Decisions in milliseconds. Across thousands of endpoints. Every action attributed in real time to the agent, model, or human that caused it.

03 / THE PRODUCT — One sensor. Total endpoint software control.

Scout
SCANNER · AGENTLESS

Agentless. Read-only. Deploys in minutes.

- Full inventory of agents, plugins, extensions, MCP servers, and skills
- Attack-path analysis on agent permissions and drift detection
- Risk report your team can act on the same day

Sense
SENSOR · RUNTIME

Everything in Scout, plus real-time policy enforcement.

- Human vs. agent attribution in real time
- Enforcement on tool calls, API access, and data movement
- Application control across binaries, scripts, MCP servers, and extensions
- Integrates with SIEM, SOAR, IdP. No kernel module required

04 / POLICY ENGINE — One rule. Four dimensions. Every software class.

WHO	WHAT	WHERE	HOW
Any Agent	**Read .env**	**Engineer's Mac**	**Require Human**
Copilot, Claude, custom, or human user	Secrets, tokens, keys, PII, source	Managed or unmanaged, on or off network	Block, allow, or hold for approval

● ENFORCED

"No agent on any endpoint may access credentials, push code, or call external tools without human approval."

"Within fifteen minutes we found AI agents with admin permissions no one on my team had approved. Neo showed us a layer we simply were not monitoring, and gave us a way to enforce policy on day one."

CISO, GLOBAL MANUFACTURING ENTERPRISE

ARCHITECTURE REVIEW

See what is hiding in your environment.

A working session with our security architects. Your stack reviewed. Coverage gaps identified. Next steps clear.

Neo.security info@Neo.security

< 15 min
First scan to full inventory

Zero
Impact on endpoint performance

Hours
Full deployment with IdP and SOC