

Exeon.AgentGuard

Behavioral threat detection across AI interactions.

AI agents gain access faster than security teams gain visibility. Assistants and autonomous agents can access company data, call tools, and act through valid permissions.

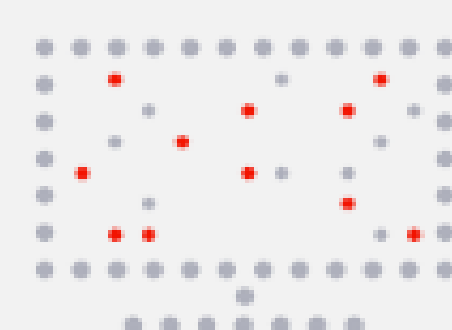
Exeon.AgentGuard analyzes AI interactions to **flag potential data leakage and detect risky agent behavior.**

What you gain with Exeon.AgentGuard



Summarize AI agent activities

Understand which models, tools, and resources agents use, with summaries and relevant account context.



Inspect agent and user activity live

Review detailed agent and user activities, including instructions, tool calls, file actions, and data flows, to investigate risks.



Detect data leakage from agents

Surface sensitive data in agents' outgoing prompts and files. Investigate external destinations and unusual data volumes.



Detect malicious agent behavior

Flag rogue agents that deviate from expected behavior or perform unsafe actions using legitimate permissions.

Trusted by

Why act **now**



AI agents exceed their boundaries

53% of surveyed organizations report that AI agents exceed intended permissions occasionally.

Source: Cloud Security Alliance, April 2026



AI incidents expose data

60% of AI-related security incidents result in the compromise of sensitive information.

Source: IBM, CDBR, July 2025



AI oversight is lagging

63% of breached organizations had no AI governance policy or were still developing one.

Source: IBM, CDBR, July 2025

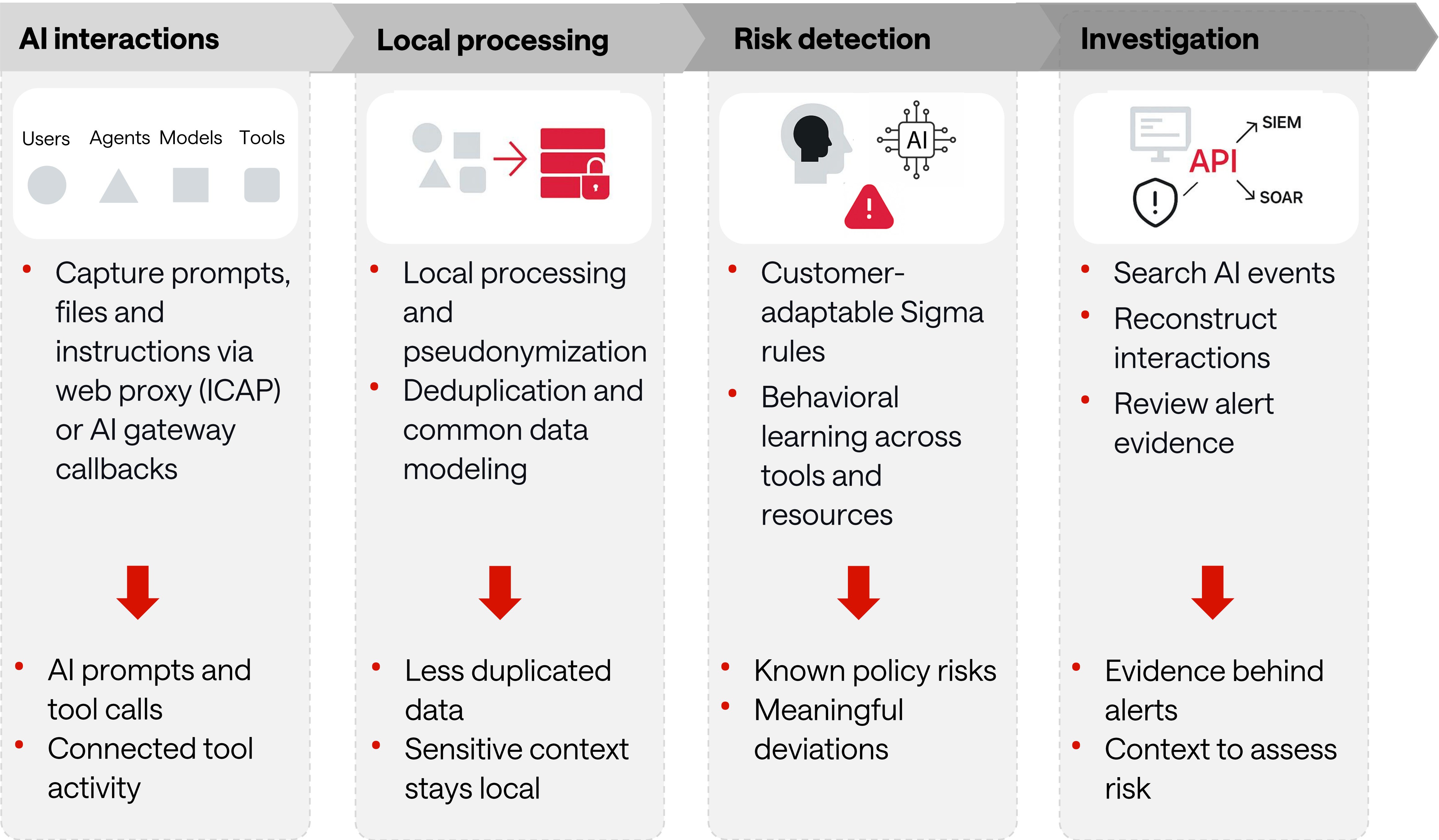


Agent activity is hard to trace

Only 12% of respondents can consistently trace every agent's actions from initial instructions through tools and APIs to outcomes.

Source: Salt Security, October 2026

How **Exeon.AgentGuard** works



Interested in **Exeon.AgentGuard**?



Exeon Analytics AG

exeon.ai

+41 44 500 77 21

contact@exeon.com



