

Solution Brief

How Oligo Secures AI-Powered Applications






AI Adoption Brings New Risks

Organizations are adopting AI rapidly, but this technological breakthrough both accelerates existing risks and introduces new ones.. These include:

- 1 Lack of visibility into agentic activity:** the SANS Institute reports that 45% of organizations cannot track autonomous AI or agentic behavior, making it difficult to detect policy violations or malicious actions.
- 2 AI-Generated code introducing new vulnerabilities:** research shows that only 55% of AI-generated code passes security reviews, with frequent flaws including injection risks, buffer overflows, and inadequate input validation.
- 3 AI tool sprawl increases the attack surface:** the use of AI tools is skyrocketing. 88% of enterprises now spend more than 5% of total IT budget on AI (EY), and this figure is expected to rise significantly.

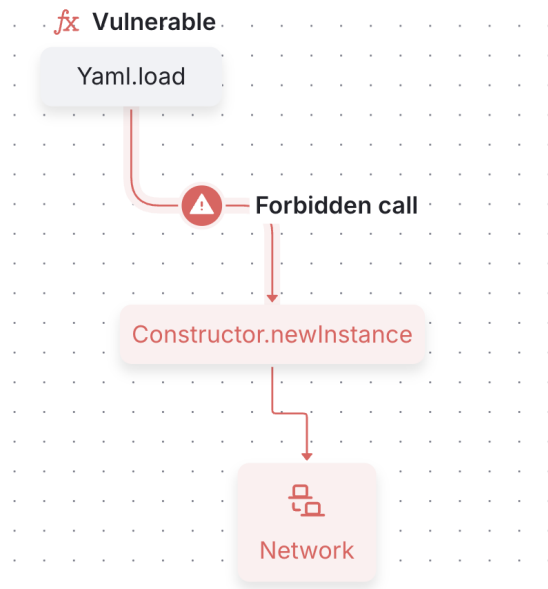
Oligo Solution: Runtime Security for AI

Oligo provides runtime protection and governance for AI workloads, ensuring security teams can detect and respond to real threats, *not just theoretical ones*.

-  **Discover AI Components in Use:** identify libraries, frameworks, and dependencies active in runtime.
-  **Detect Zero-Day Exploits:** spot exploitation attempts against AI technologies in real time.
-  **AI Threat Detection and Response (AI-DR):** monitor autonomous AI actions for unsafe or unintended behavior.
-  **Secure Inference Servers:** protect the execution stack of LLMs and inference environments.
-  **Defend AI Supply Chains:** detect and block compromised AI packages in production.
-  **Risk Reporting & Compliance:** map AI risk exposure for governance.




Security Use Cases

- Protect inference servers at runtime
- Gain runtime visibility into risks
- Detect active exploitation, including zero-days
- Monitor & control agentic AI behavior



Developer Use Cases

- Ship AI features with safe dependencies
- Identify which components are safe for production
- Receive actionable remediation without slowing releases

| Dependency@ver ↑ | Image build ID | Import type | Runtime status | Public fix |
|------------------|--|-------------|--|---|
| torchserve@0.8.0 | # df5bd6  | ➡ Direct |  Executed |  Not fixable |

Why Oligo?

- ✓ **Agentic AI Oversight:** Detects unsafe or unintended actions by autonomous agents.
- ✓ **AI Security Expertise:** Research team behind ShadowRay and MetaLlama vulnerability discoveries.
- ✓ **Runtime Focus:** Unlike static scanners, Oligo observes real execution and behavior.
- ✓ **Zero-Day Threat Detection:** Oligo identifies exploitation patterns before public disclosures.