

EVO BY SNYK

AI Security for an Agentic World.

The AI era is reshaping how software gets built, deployed, and attacked. Evo by Snyk is the AI Security Platform for an agentic world — securing the code AI writes, the agents it runs, and the applications it builds. Through Agentic Development Security (ADS), AI-SPM, and Continuous Offensive Security (COS), Evo helps organizations adopt AI with confidence across the full software lifecycle.

The security gap is real - and it's growing.

AI is moving faster than the controls built to govern it. Three gaps have opened up simultaneously.

- Development is outside the loop. AI agents write insecure code, use unvetted tools, and operate with excessive access at machine speed - outside the reach of traditional AppSec controls.
- AI adoption is invisible to security. Models, agents, and AI services are deployed across every team without a unified inventory, consistent policy, or governance layer.
- The attack surface has changed. Testing hasn't. AI introduces new vulnerability classes - prompt injection, agent hijacking, model manipulation - that periodic pentests weren't built to find.

Evo closes all three gaps - in one platform.

Evo is purpose-built for this new reality, with a solution for each dimension of AI risk.

- **Secure the AI workforce powering modern development. Evo Agentic Development Security (ADS)** secures what agents use, do, and generate — helping organizations safely scale AI-driven software development.
- Gain total visibility and machine-speed governance for AI applications. **Evo AI Security Posture Management (AI-SPM)** provides a live AI-BOM of assets, risk intelligence, and policy enforcement across models, agents, workflows, and applications.
- Continuously validate deployed systems through AI-native offensive security. **Evo Continuous Offensive Security (COS)** uses AI-powered pentesting and agent red teaming to uncover exploitable vulnerabilities before attackers do.

Every organization building with AI must answer one question:
can we trust what we're shipping?

PROTECTED BY SNYK



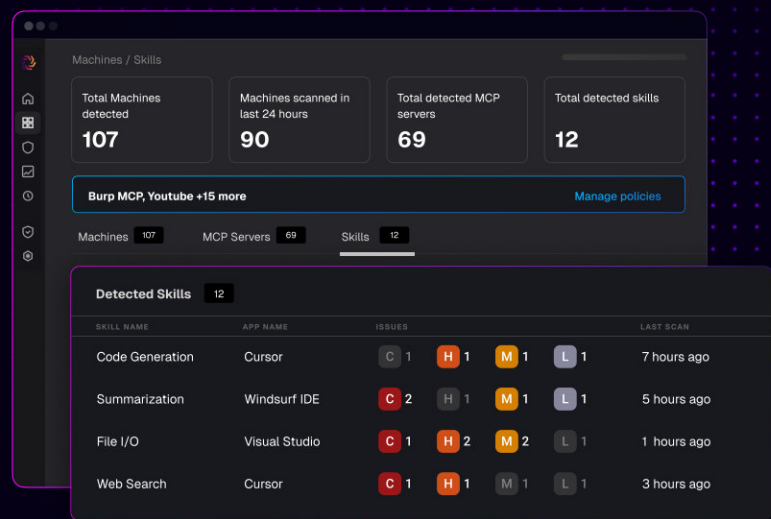
Evo Agentic Development Security (ADS)

Secure the AI workforce powering modern development

AI agents are now writing code, invoking tools, and executing workflows at machine speed — becoming a critical part of the AI workforce powering modern software development. Traditional AppSec controls sit outside these workflows. By the time code reaches a scanner, dozens of ungoverned decisions have already been made. Evo ADS operates directly inside agent workflows, giving organizations visibility and control across what agents use, what they do, and what they generate.

What Evo ADS secures:

- **The agent supply chain** - Discover and govern MCP servers, tools, skills, and dependencies before they enter agent workflows.
- **Agent behavior** - Enforce policy inside the execution loop. Block or modify unsafe actions using full session and intent context.
- **Agent output** - Analyze and secure AI-generated code at the moment of creation, using Snyk's trusted security intelligence.



"We're seeing supply chain attacks, malicious skills, and compromised MCP servers riding in on the agent's own toolchain, plus agents taking actions with no guardrails between intent and execution. Working with Snyk, we landed on what I think is the right agentic development security architecture: controls built directly into the agent workflow that govern what an agent uses, executes, and generates."

BRENDAN PUTEK, DIRECTOR OF DEVOPS, RELAY NETWORK

Evo AI Security Posture Management (AI-SPM)

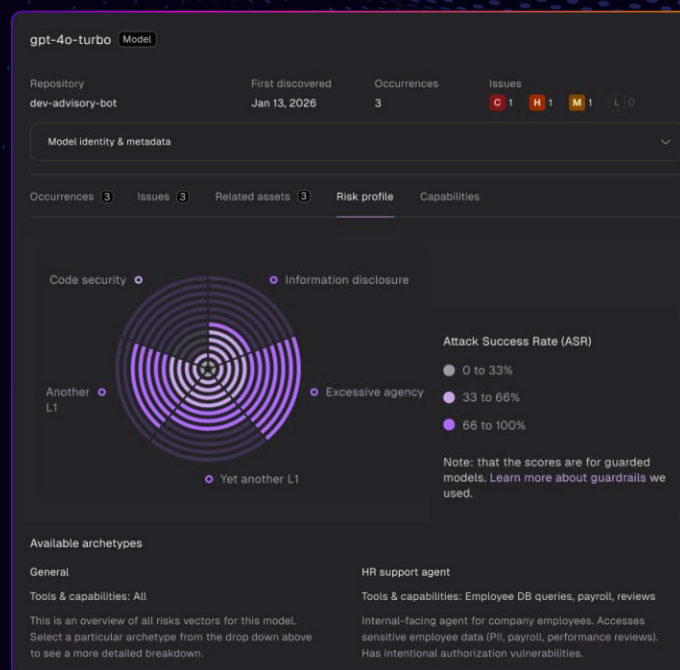
Total visibility and machine-speed governance for AI applications

AI makes decisions at runtime that traditional security tools never see. Models choose tools, agents take actions, and MCP servers execute work all in environments where most organizations can't answer a basic question: what AI is actually running in our production environment?

Evo AI-SPM gives you the visibility to know what's running, the forensics to understand what happened, and the enforcement to ensure it never happens again.

What Evo AI-SPM governs:

- **Discover shadow AI** - Automatically discover every model, agent, MCP server, and dataset across your repositories and environments, with a live AI-BOM tracking for every component in use.
- **Assess risk exposure** - Agent data mapping to show what applications and agents touch which data sources, via which models and tools, so security teams know where to look when something goes wrong.
- **Define policy guardrails** - Define in plain language which AI tools and models are approved, flag violations, and enforce controls automatically - across every team and environment.



"One of the things that was exciting about Evo AI-SPM is the visibility. It only took an afternoon to set it up and less time to pull a report and have full visibility. Here at WEX, we take a business-impact approach to AI. Being able to put our arms around the full breadth of what was actually in place was a super helpful foundation to start from."

JASON LANGSTON, DIRECTOR, PRODUCT SECURITY AT WEX

EARLY ACCESS

Evo Continuous Offensive Security (COS)

Proactive defense through AI-native offensive security testing.

AI-generated code and AI-native applications are expanding the attack surface faster than traditional pentesting can keep up. Security teams need a way to continuously identify exploitable risk — not just theoretical findings. Evo Continuous Offensive Security uses reasoning-capable AI to continuously test applications the way attackers do — uncovering exploitable vulnerabilities as systems evolve.

What EVO COS covers:

- **Find what others miss** - Surface business logic flaws, BOLA, privilege escalation, authorization weaknesses, and chained attack paths that traditional scanners cannot detect.
- **Continuous, not point-in-time** - Continuously tests meaningful application changes so offensive security keeps pace with development and attacker activity.
- **Built for modern applications** - Uses reasoning-capable AI to simulate real-world attacks against AI-native and traditional applications, validating what is genuinely exploitable. A dedicated validation model acts as an independent judge, confirming exploitability before any finding surfaces.
- **Powered by Snyk platform intelligence** - COS uses findings from SAST, SCA, DAST, and application context to focus testing on what is most likely to be exploitable.

Interested in early access? Talk to your Snyk rep.

Built into every Evo solution.

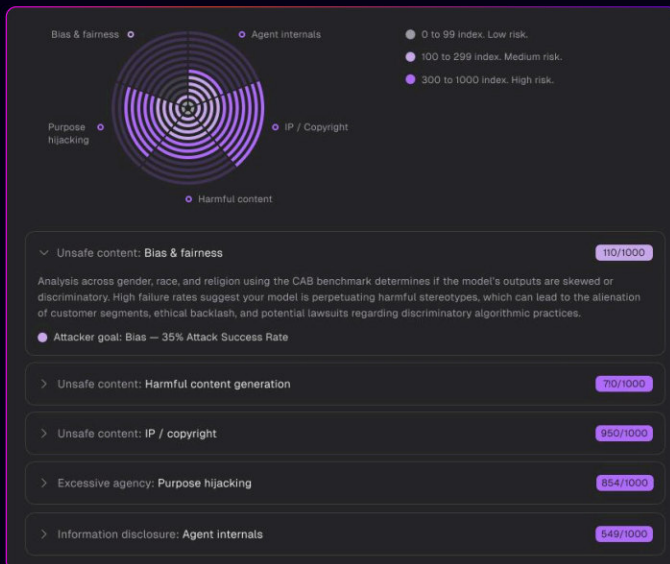
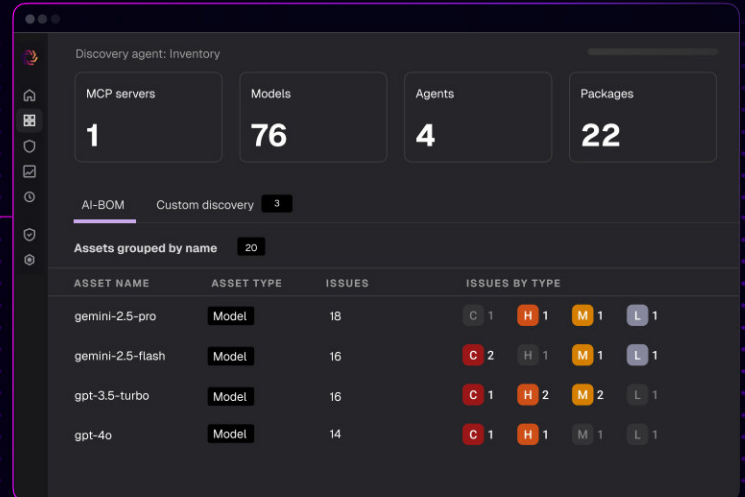
Evo isn't a collection of standalone tools. Evo orchestrates every workflow across ADS, AI-SPM, and COS, with each solution powered by the same platform intelligence, agents, and governance capabilities underneath.

"We're seeing supply chain attacks, malicious skills, and compromised MCP servers riding in on the agent's own toolchain, plus agents taking actions with no guardrails between intent and execution. Working with Snyk, we landed on what I think is the right agentic development security architecture: controls built directly into the agent workflow that govern what an agent uses, executes, and generates."

BRENDAN PUTEK, DIRECTOR OF DEVOPS, RELAY NETWORK

Discovery

Automatically discovers every AI asset including models, MCP servers, agents, skills, and datasets — across your code and developer machines, in one always-current inventory.



Risk intelligence

Evo continuously tests models across real-world agentic archetypes, chatbots, code assistants and produces the empirical attack success rate. That intelligence flows into every policy you create, every agent you trust, and every deployment decision you make. Gain risk signal capabilities across Evo solution - prioritized by exploitability, asset criticality, and business context.

Agent orchestration

Evo uses AI agents to secure AI systems. Under the hood, Evo capabilities run continuously across your repositories and environments, detecting drift, evaluating context, and enforcing policy without waiting for a human to trigger a rescan. This coordination happens within a conversational chat to help drive control by explaining, and acting on the user's behalf.

Two more worth flagging for a different reason (Insecure Code Generation):

- **claude-sonnet-4-20250514** — Code Gen: **782**. Very likely to produce vulnerable code despite having a lower safety index.
- **gpt-4o** — Code Gen: **773**. Same pattern.
- **meta-llama/meta-llama-3-8b-instruct** — Bias: **1000** (maximum). Extremely high discriminatory output risk.

Asset Inventory

The table above shows all models, datasets, and MCP servers across your repos with vendor, license type, and country of origin.

Policy

A **critical** policy "Block High-Risk Models (Safety Guardrail Bypass $\geq$ 400)" is ready for review in the UI. It will flag any model with a Safety Guardrail Bypass index at or above 400, which immediately catches **gpt-3.5-turbo** and **gemini-2.5-flash** as violations.

If you want additional policies covering the code generation risk ($\geq$ 700) or the bias outlier (Meta-Llama at 1000), I can prepare those in parallel as well.

Review high-risk models list

Create blocking policy now

Check related datasets

Issue management

Every issue in Evo is generated automatically the moment a policy match is detected. No manual scans, no scheduled tests, no waiting for the next scheduled review to find out what's risky. Findings from across Evo's solutions flow into a unified issue management layer. Tracks, prioritizes, and routes the issues capabilities raise such as status, severity, ownership, lifecycle into existing workflows (tickets, CI/CD, reports)

Critical	High	Medium	Low
36 issues +33	75 issues +67	130 issues +120	0 issues

Policies: 18 Issues: 75 Create policy				
Q Search...				
Asset name	Repository name	Policy name	Severity	Occurrences
gpt-4	snyk/maverick	Bias & Discrimination	High	18
gpt-4	snyk/maverick	Block openAI models	High	18
gpt-4o	snyk-labs/ai-bom-goof	Block openAI models	High	17
gpt-4o	snyk-labs/ai-bom-goof	Insecure Code Generation	High	17
gpt-3.5-turbo	christatimer/microagent	Safety Guardrail Bypass	High	15
gpt-3.5-turbo	christatimer/microagent	Block openAI models	High	15
gpt-3.5-turbo	snyk/maverick	Safety Guardrail Bypass	High	12
gpt-3.5-turbo	snyk/maverick	Block openAI models	High	12
gpt-5	oana-sipos/...ime-copilot	Block openAI models	High	7
claude-opus-4-6	mozilla/bugbug	Insecure Code Generation	High	7

Governance and policy

Evo translates organizational intent into enforceable, audit-ready security guardrails. Define policies in plain language, and Evo translates it into an active policy immediately, enforced globally across dev, staging, and runtime with five Snyk-authored default policies covering the highest-impact risks from day one. No spreadsheets. No manual approvals. No bottlenecks.

Issues triggered by the Block Chinese Models policy

Download as CSV

Results: 8

Q Search...

Asset name	Asset type	Severity	State	Asset vendor	Asset country of origin	Policy name
deepseek-v2	Model	High	Open	DeepSeek		
deepseek-reasoner	Model	High	Open	DeepSeek		
deepseek-v2	Model	Critical	Open	DeepSeek		
deepseek-reasoner	Model	Critical	Open	DeepSeek		
deepseek-v2	Model	High	Open	DeepSeek		
deepseek-llm-67b-chat	Model	High	Open	DeepSeek		
deepseek-ai/DeepSeek-V2	Model	High	Open	DeepSeek		
deepseek-reasoner	Model	High	Open	DeepSeek		

Cancel

Evo

you like to do today?

Create a policy that blocks all chinese models

The policy is ready for review with these settings:

- Name: Block Chinese Models
- Severity: High
- Condition: Asset type = Model AND Country of origin = China (CN)
- Remediation: Replace with an approved model not originating from China

Review the pre-filled form and save when you're ready.

Show issues related to blocked Chinese models

The table above shows all open issues triggered by the "Block Chinese Models" policy, including each violating asset's name, type, vendor, and country of origin.

View Block Chinese Models policy

Filter critical severity issues

Create policy for deepseek-v2

By the numbers

- 65–70% of production code is now AI-generated, and nearly half contains vulnerabilities. (Snyk 2026 State of Agentic AI Adoption Report; corroborated by BaxBench, ETH Zurich.)
- 50.8% of developers have MCP server connections configured. 28% of skills expose agents to third-party content (Snyk Inside the Agentic Development Supply Chain Report.)
- 52% reduction in mean-time-to-remediation and 60% faster vulnerability remediation. (Forrester TEI.)
- 288% ROI and \$15.5M NPV over three years. (Forrester TEI.)
- 4,800+ enterprise environments inform Snyk's ground truth.

Can we trust what we're shipping?

Every organization building with AI needs to answer one question: can we trust what we're shipping? Snyk is how you architect that answer — securing the code AI writes, the agents it runs, and the applications it builds. Evo delivers that answer across the AI software lifecycle, with visibility, governance, and continuous validation.

[Get a demo](#)

snyk