opentext™

Agentic AI changes AppSec risk

AI is no longer just writing code—it's deciding, acting, and deploying faster than humans can intervene.

In 2026, **40%** **of net-new applications are AI-driven**,[1] introducing machine-speed decisions across software delivery.

From code to autonomous action

Agentic AI doesn't just assist developers, it decides, executes, and adapts without human approval.

Autonomous agents can chain actions across CI/CD pipelines, cloud infrastructure, and security tools—operating continuously, not episodically.

Risk accelerates at machine speed

Autonomous agents can repeat actions instantly, scaling mistakes, misconfigurations, and vulnerabilities across systems in seconds.

As of 2024, 17% of organizations had GenAI applications in production, with another 38% investing[1]—often before governance models are fully mature.

Built for humans. Broken by agents.

Traditional AppSec controls assume predictable workflows, static permissions, and human checkpoints.

Agentic systems constantly change behavior, context, and access—breaking those assumptions.

65% of engineering leaders report teams already using AI tools.[2]

76% of organizations restricting AI cite security risk as the reason.[2]

The new AppSec question

Old question: Did we scan the code?

New question: Can we govern autonomous behavior—continuously?

Organizations that treat AI agents as secure, observable digital actors gain speed without losing control.

Build guardrails that let AI move fast—without losing control

AppSec-focused controls for building AI and agentic AI applications securely.

Download the AI Application Security Checklist

IDC, *The Peril and Promise of Generative AI in Application Security*, July 2024

Gartner, *Application Security Strategy 2026: AI, DevSecOps and Platform Consolidation*, September 2025

opentext™