OpenText Application Security Aviator

AI-augmented SAST for faster, smarter secure code review

Benefits

- Reduce false positives with high-accuracy AI triage
- Describe findings with clear, source-aware explanations
- Enable tailored remediation workflows across dev and security teams
- Boost developer productivity while improving trust in SAST

Fixing security flaws is harder than ever. Development teams today face growing codebases, faster release cycles, and limited resources. Traditional static analysis tools often overwhelm developers with an avalanche of false positives, each requiring extensive triage, research, and remediation. The result: wasted time, reduced productivity, and a constant bottleneck that slows innovation. OpenText Application Security Aviator uses large language models (LLMs) to highlight real issues, explain them clearly, and accelerate secure development. Aviator applies AI to enhance static analysis—not to detect LLM-specific threats or AI-generated code vulnerabilities, but to improve the clarity and efficiency of secure code reviews.

Reduce noise and alert fatigue

Security teams often spend too much time reviewing static analysis results that don't matter. Aviator reduces that burden by automatically classifying issues with high accuracy, cutting down on false positives and helping teams focus on real vulnerabilities.

With clear, source-aware explanations in the developer's language, developers and analysts see why an issue was flagged and what to do next, saving time on follow ups and manual validation.

Speed up remediation with practical guidance

When a real issue is found, Aviator provides clear context and remediation help. It explains the problem in plain language and, when possible, offers targeted, language-specific code suggestions that fit the issue.

This shortens the time from detection to resolution and supports smoother collaboration between security and development teams, whether during early testing or right before release.

OpenText Application Security Aviator deployment options

Accelerate cloud strategies with OpenText cloud experts

- OpenText Managed Private Cloud

Extend your team

- On-premises software, managed by your organization or OpenText

Run anywhere and scale globally in the OpenText public cloud

- SaaS: Aviator runs in the OpenText Public Cloud, delivered as a service

Run anywhere and scale globally in the hyperscaler cloud of your choice

- AWS, Azure, GCP, or OpenText Private Cloud

Resources

OpenText Application Security Aviator
Learn more ›

Why SAST false positives are inevitable
Read the blog ›

Fortify Audit Assistant Documentation
Learn more ›

OpenText Cybersecurity
Join the community ›

Built for scale and continuous delivery

Aviator integrates into CI/CD pipelines to support security at scale. By verifying issues directly in source code, it improves the accuracy of SAST without slowing down the build process. It's designed for teams handling large codebases, multiple repositories, or fast-paced release cycles—helping streamline triage and keep your AppSec program focused and efficient.

OpenText Application Security Aviator reduces false positives, saves developers time, and improves the clarity and accuracy of secure code reviews. It brings consistency and structure to static analysis, helping teams keep up with the speed and scale of modern development.

While AI introduces new risks across the SDLC, Aviator is focused on using AI internally to improve the precision and usability of static analysis—not to detect threats introduced by AI-generated code. Unlike generic AI integrations, Aviator is built directly into the OpenText AppSec platform to enhance static analysis precision and streamline workflows end to end.

Feature	Description
AI-powered static analysis auditor	Leverages large language models (LLMs) to automatically audit static scan results with high precision and minimal false positives.
Context-aware remediation guidance	Delivers accurate, copy-ready code fixes along with rationale, helping developers resolve issues faster.
Human-readable explanations	Provides plain-language justifications for audit decisions to boost clarity and trust across security teams.
Automated triage in CI/CD	Integrates directly into development pipelines, reducing manual review cycles before issues reach humans.
False positive suppression Engine	Identifies and suppresses likely false positives to focus teams on actionable vulnerabilities.
Broad language coverage	Supports scanning results across 30+ programming languages, accommodating diverse enterprise codebases.
AI-driven issue tagging	Automatically classifies findings with audit tags to support compliance workflows and streamline remediation.
Secure-by-design enablement	Complements secure development practices by aligning with developer enablement and secure coding tools.
Seamless platform integration	Embedded within OpenText Application Security Center and orchestrated through ScanCentral for unified operations.
Flexible delivery models	Available in SaaS and self-managed deployments, supporting hybrid and regulated environments.

opentext™