OpenText Application Security Aviator

Use AI to cut false positives, streamline remediation,
and elevate the ROI of your AppSec program

Benefits

- Cut time-to-remediate from days to hours
- Increase trust in SAST accuracy
- Reduce AppSec backlog with AI triage
- Strengthen collaboration across AppSec and dev teams
- Shrink MTTR from days to minutes with auto-remediation"

OpenText™ Application Security Aviator™ uses advanced large language models (LLMs) to transform how static application security testing (SAST) works. Rather than flooding teams with alerts, Aviator intelligently audits scan results, suppresses false positives, and delivers clear, context-rich explanations and fix recommendations—at scale. And with new auto-remediation, Aviator can apply validated fixes, shrinking repetitive, manual remediation timelines from days to minutes

It turns traditional SAST into a signal-based system, giving AppSec leaders the clarity to prioritize risk, the speed to respond quickly, and the accuracy to trust in results.

Reduce software security risk faster

Aviator dramatically reduces mean time to remediate (MTTR) by eliminating noise and helping developers fix issues directly in their workflow—with precision, not guesswork.

Improve ROI on AppSec investments

By lowering triage overhead and enhancing SAST accuracy, Aviator helps organizations get more value from their existing Fortify infrastructure and developer resources.

Strengthen secure DevOps at scale

Aviator integrates directly into CI/CD pipelines, giving security leaders visibility into actual risk, not just raw scan volumes, and enabling action before releases go out the door.

Prove security maturity and impact

With explainable, traceable results and suppressed false positives, Aviator gives AppSec leadership the data and clarity needed to report confidently to executives and boards.

OpenText Application Security Aviator brings strategic clarity to static analysis. It enables AppSec teams to do more with less—less manual triage, less noise, less friction—while delivering faster remediation and greater accuracy.

Backed by more than a decade of AI and security innovation, Aviator turns your existing SAST program into a scalable, AI-enhanced risk reduction engine that supports business outcomes, not just code reviews.

- **AI-driven SAST triage engine** - Automates issue classification to reduce false positives and accelerate real risk resolution.
- **Contextual code fix suggestions** - Reduces remediation time by guiding developers with accurate, role-relevant fix recommendations.
- **Developer-ready explanations** - Builds trust with source-aware, natural language explanations that improve collaboration and speed.
- **Auto-remediation** - Automatically generates and applies validated fixes to eligible findings to reduce repetitive work and shrink exposure windows.
- **Seamless CI/CD integration** - Fits directly into automated pipelines to support secure DevOps and shift-left strategies.
- **Enterprise deployment flexibility** - Available as SaaS or self-managed, supporting cloud, hybrid, and regulated environments.
- **Governance-aligned suppression** - Suppresses low-risk findings with configurable false-positive auto suppression and traceable logic.
- **Server-side orchestration** - Lets security teams enable Aviator organization-wide without developers updating local tooling.
- **Broad language & category coverage** - Analysis across more than 33 languages and more than 1,500 vulnerability categories to deliver precise, contextual guidance.

opentext™