VERACODE

DATASHEET

Veracode Fix

AI-Powered Automated Remediation for Custom and Open-Source Code

Generative AI is compressing weeks of development into days — and producing security debt faster than teams can review, scan, or fix it. Code volume is rising roughly one-third per sprint in organizations using AI assistants. Even when the defect rate per line stays flat, that means more code to scan and more flaws to remediate. AI-generated code often includes hallucinated logic, bloated structures, and unchecked third-party dependencies, expanding the attack surface while review capacity stays the same.

Take Control with Veracode Fix

Veracode Fix is an AI-powered remediation solution that proactively identifies flaws and automatically generates secure code fixes — for both first-party custom code and third-party open-source dependencies. Forged from decades of application security expertise, it accelerates remediation and cuts risk without taking developers out of their workflow.

243 Days

Average fix time for software security vulnerabilities.

Veracode SoSS 2026

Why Veracode Fix?

- **Responsible AI, Not Generalist Code Gen:** Trained on millions of human-verified reference patches — not general-purpose training data prone to flaws, IP issues, or model poisoning. Generated fixes address the root-cause vulnerability class, not just the scanner finding.
- **Proprietary, Expert-Validated Data:** Built on a highly curated dataset of secure patches reviewed by Veracode's Threat Research Team. The validation mechanism is the differentiation — fixes are backed by human security reviewers, so they don't introduce new security debt.
- **Human-in-the-Loop Trust:** AI suggests fixes; developers review and approve. No fully autonomous remediation pushed to production — the control stays with the team.
- **Unified SAST + SCA Coverage:** One solution for both first-party code flaws and third-party dependency vulnerabilities, closing the gap between code remediation and supply-chain remediation.
- **Proven Impact:** ~80% fix rate, 200% improvement in mean time to remediate, and 92% reduction in flaw detection time across supported languages.

KEY USE CASES & BENEFITS

- **Burn Down Security Debt:** Automated, context-aware fixes integrated into developer workflows let teams systematically reduce backlogs of custom-code and open-source vulnerabilities.
- **Accelerate Remediation:** Fix security flaws in minutes, not months — without context switching or disrupting developer workflow.
- **Scale Security Across the SDLC:** Tackle critical vulnerabilities automatically across languages and ecosystems, keeping pace as code volume grows.
- **Reduce Business Risk:** Remediate critical flaws automatically, significantly decreasing overall risk exposure and potential for security incidents.
- **Empower Developer Teams:** Tight integration into existing toolchains (CLI, IDE, SCM) drives adoption and improves productivity.

Veracode Fix

Save time with AI-Powered Automated Code Remediation.

Veracode Fix for SAST: Remediate Code Smarter with AI

Automatically generates secure code fixes for flaws in first-party custom code, turning static analysis findings into ready-to-apply patches that reduce MTTR and burn down backlogs

- **AI-Generated Secure Code Fixes:** Resolves flaws with high accuracy across multiple languages (e.g., 3-out-of-4 Java static findings).
- **Batch Fix:** Bulk remediation across files in one CLI operation, ideal for scalable fixes like sanitizers.
- **IDE Integration:** Real-time fixes in VS Code (IntelliJ, PyCharm, Eclipse in development), keeping context intact.
- **Comprehensive CWE Coverage:** Targets prevalent vulnerabilities (CWE-80, CWE-89, CWE-117), addressing 92% of critical open flaws.

How It Works: Veracode static analysis detects a flaw → trusted AI trained on curated Veracode patches analyzes it → produces a secure patch (e.g., URLEncoder for log sanitization) → developers apply via CLI or IDE → fixes integrate into workflows, reducing security debt and MTTR.

Supported Languages: Java, C#, JavaScript, TypeScript, Python, PHP, Scala, Kotlin, Ruby. Integrations: Static Pipeline (GA), Static IDE (GA), Static Policy (Post-GA), CLI, VS Code. Batch Fix Restrictions: Excludes CWEs 311, 312, 327, 73, 502, 601 in batch mode.

Veracode Fix for SCA : Automated Remediation for Open-Source Security

Automatically generates ready-to-merge pull requests that upgrade vulnerable open-source libraries to secure versions — while analyzing the impact on first-party code to prevent breaking changes.

- **Automated, Context-Aware Pull Requests:** Generates ready-to-merge PRs suggesting the optimal secure library version while minimizing the risk of breaking builds.
- **Contextual Analysis of First-Party Code:** Prevents breaking changes and ensures application stability by analyzing the impact of library updates — handling both the dependency update and any first-party code changes required to avoid build breaks.
- **Proprietary Vulnerability Database:** Built on Veracode's industry-leading vulnerability database, curated by an in-house security research team, for accurate and comprehensive intelligence.
- **Integration with Developer Toolchains:** Fits into existing Git-based workflows (GitHub, GitLab), enhancing productivity and driving adoption.

How It Works: Veracode SCA detects a vulnerability in an open-source library → Fix analyzes it, cross-references the proprietary database, and evaluates upgrade impact on first-party code → generates a PR with the optimal secure version → developer reviews and merges → vulnerability fixed in minutes with minimal disruption.

Supported Scans: SCA Agent-Based Scans. Integrations: CLI, Source Code Management (SCM): GitHub, GitLab, and other Git-based systems.

CAPABILITY	FIX FOR SAST (CODE REMEDIATION)	FIX FOR SCA (DEPENDENCY REMEDIATION)
Primary goal	Fix code flaws fast with AI assistance	Fix vulnerable open-source dependencies fast with PR-based remediation
Object being fixed	First-party source code findings	Third-party libraries + transitive dependencies (supply chain risk)
Where the work happens	IDE, CLI, CI/CD (interactive + batch)	SCM pull requests (reviewable PRs) + workflow integrations
Output artifact	AI-generated fix suggestions (applied by developers)	Evidence-rich pull request with rationale and supporting references
Coverage	On average, covers over 70% of detected flaws in 10 supported languages	Supported ecosystems (contact for the complete, current list)
Trust model	No place for hallucinations; inbuilt quality gates; does not retain customer code	Human-in-control via PR review + approval gates; auditability built in
Breaking change risk	Quality gates help ensure reliable suggestions	Explicitly designed to minimize breaking changes and protect first-party code stability
Rollout controls	Interactive + batch modes to fit team workflows	Suggest-only/audit mode before enforcement
Best-fit stakeholders	Developers + AppSec teams reducing code security debt	AppSec + Vulnerability Mgmt + Compliance leaders needing controlled, auditable remediation

Contact Us

Contact us today to learn more about how Veracode Fix can help you reduce risk and secure your application security. Contact our team at www.veracode.com schedule a demo or request additional information.

VERACODE