Veracode Fix and the Future of Intelligent Software Security

Using artificial intelligence to help organizations defend against application security threats with speed, accuracy, and efficiency.

What if you could **fix 74% of Java static analysis findings** without writing a single line of code?

Introduction

Building on the past to create a safer future

Software development and security teams have been sprinting just to stand still. For years, software security has revolved around testing to find issues. But for every issue found, there is a manual task to fix. DevOps automation and improved detection created an imbalance between how efficiently flaws are created and found verses how effectively they are fixed. This imbalance has led to accruing security debt, alert fatigue, and longer development cycles.

Developers are often tasked with spending time they don't have, fixing security flaws they don't understand, in code they didn't create... only to find in the time it takes to fix one flaw, two more are created elsewhere.

The need for transformation is evident.

Veracode Fix delivers that transformation, shifting the paradigm from find to fix and marking the advent of intelligent software security. By harnessing the power of Artificial Intelligence ("AI") to automatically generate fixes for insecure software, Veracode Fix finally brings automation to flaw remediation and re-balances the software security landscape.

For 17 years, Veracode has built trust in new and innovative technologies. We pioneered application security testing as a SaaS solution and are continuing that legacy with Veracode Fix as an example of responsible AI in practice. Unlike most generative AI coding tools, Veracode Fix is not trained on open-source code or code in the wild and does not use or retain customer data to train the model.

Instead, we trained Veracode Fix on a proprietary, curated dataset with supervised learning and alignment from our team of leading security researchers and application security consultants to deliver Veracode's aggregate experience and expertise in a simple, powerful experience: the power of Veracode at your fingertips.

All images in this document were created using AI.

The Problem:
Too much time. Too little security.

Developers and security teams spend too much time and effort to achieve too little from a security perspective. They struggle to manage the risk of intensifying threats against an expanding attack surface while accelerating development velocity and minimizing costs. This is because, despite automation in the software development process and flaw detection, fixing security findings – particularly in first-party code – has relied on manual effort from overburdened and under-supported developers. Until now.

Flaws are found and created faster than they can be fixed.

Development teams cannot keep pace with security debt and create new flaws faster than they can fix old ones.

DevOps, automation, and AI companion coding make developers more and more productive... at producing insecure software. And while developers have gotten better at finding flaws, fixing them remains a manual effort.

This results in accumulating security debt and increasing operational risk and costs.

Accruing security debt leads to greater risk and higher costs.

Accumulating security debt creates more operational risk, requires more resources to address, and jeopardizes the ability to create – and protect – revenue and value.

Like financial debt, it is a cost that can be deferred only so far before it causes strategic and/or financial crises including cybersecurity exploits, missed opportunities, failed compliance, lost revenue, inhibited innovation, inability to compete, risk to mergers and acquisitions, and more.

It is getting worse.

Flaws persist longer, accumulate faster, and lead to greater risks and costs.

Despite making it faster and easier to find flaws, time to fix is getting longer. From 2017 to 2022, the half-life to remediate static findings increased 50% to nearly 300 days. This mounts pressure on developers and security teams and adds risks for the organization.

Manual remediation simply cannot keep pace with the scale, speed, and complexity of modern software development.

The Solution:
Save time. Secure more.

Veracode Fix saves developers time and helps secure software at scale by using machine learning to generate fixes developers can review and implement without writing a single line of code. This means flaws that would otherwise persist for months can now be fixed in minutes with less effort and cost. Veracode Fix makes it possible to accelerate secure software development while defending your expanding attack surface against intensifying threats.

Save time.

Free developers to spend less time fixing and focus on delivering amazing software.

Traditionally, developers spend hours investigating a security finding, reviewing remediation guidance, and manually coding a fix.

Veracode Fix augments developers with automation. When a flaw is found with Veracode Fix support, developers can send the flaw to Veracode Fix for remediation. Veracode Fix generates one or more suggested fixes which a developer can review and implement without writing any code.

Secure more.

Remediate flaws that would otherwise take hours of manual effort and persist for months in minutes.

Development and security teams have far less capacity to fix flaws than needed.

On average, teams only address 25% of static analysis security findings per month. The majority are deferred, and it takes nearly 300 days to fix just half the flaws.[1]

Veracode Fix exponentially increases remediation capacity by generating fixes for many of the most prevalent issues – including 3 out of 4 Java static findings on average.

At scale.

Reduce risk and finally pay down your technical security debt at scale.

56% of Java applications have flat or rising security debt.[2] That means security flaws are found and created faster than they cand be fixed.

Veracode Fix makes it possible to reduce security debt by remediating existing software security flaws and prevent the introduction of new flaws by leveraging the power of generative AI and automation.

1. Veracode State of Software Security Report V12
2. Veracode State of Software Security Report 2023

How Does It Work?
Responsible AI in Practice

Overview

Veracode Fix uses machine learning to generate fixes for security flaws in custom code and vulnerable dependencies.

From a user perspective, a developer selects a flaw for remediation, Veracode Fix generates one or more suggested fixes, the developer reviews the fixes and selects one to implement as a patch, and the code is remediated without the developer needing to manually write any code.

Supported languages available now

- Java
- C#

Coming Soon

JavaScript, TypeScript, Python, C++, VB.NET, PHP, ASP.NET, Android (Kotlin/Java), Scala, iOS (Swift/ObjC), and Go RPG, COBOL, ColdFusion, Ruby, TSQL/PLSQL, and VB6

Generative AI

From a technical perspective, there are three key elements to Veracode Fix's machine learning solution:

- **The machine-learning model**: Veracode Fix uses a GPT transformer deep learning model like ChatGPT.
- **The data**: Veracode Fix is trained on a proprietary and highly curated dataset of reference patches, unlike ChatGPT or GitHub Copilot which are trained on large, un-curated datasets.
- **The training and alignment:** Veracode Fix has supervised learning and alignment from Veracode's team of expert security researchers and application security consultants.

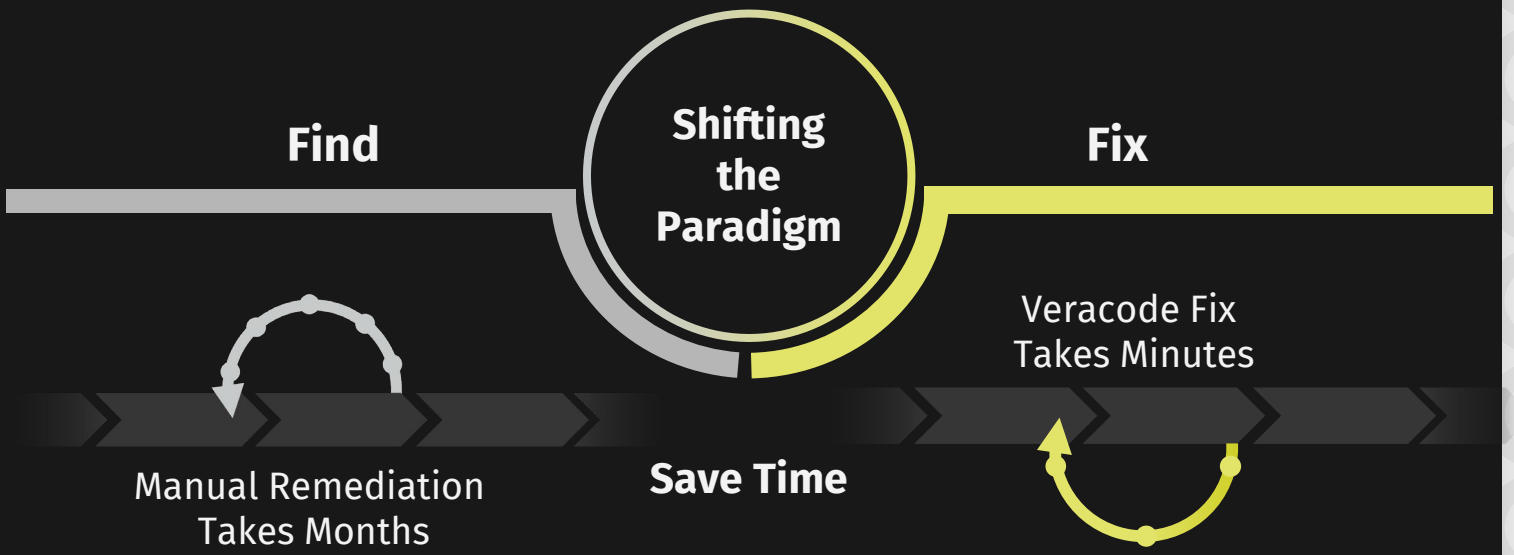
Responsible AI

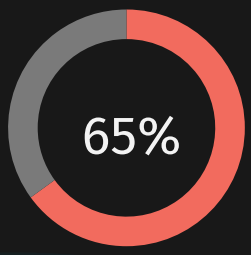
- Veracode Fix is an example of responsible AI in practice.
- Veracode Fix is **NOT** trained on code "in-the-wild" or customer code.
- Veracode encrypts customer data in transit and at rest and does not use or retain customer data to train the model.
- This differentiates Veracode Fix from other generative AI coding tools that use open-source and customer data leading to concerns and risks around code provenance.
- Veracode Fix does **NOT** automatically change or modify customers' code. A developer-in-the-loop reviews and selects suggested fixes to implement them.

The Veracode Fix Difference

Shifting the Paradigm from Find to Fix

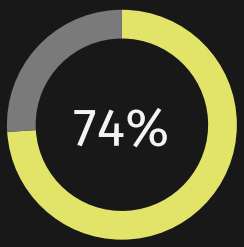
Four years ago, Veracode leadership posed the questions, "What is the most important challenge in application security?" The answer was simple - fixing security bugs. Delivering a solution to that challenge was not so simple. But after four years, an acquisition, and countless hours from an expert team, Veracode has delivered a solution that shifts the paradigm in software security from tools that only find flaws to intelligent security solutions that generate fixes.



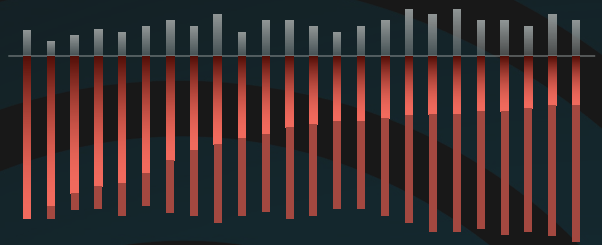


Java Flaws Still Open after 3 Months[1]

Secure More

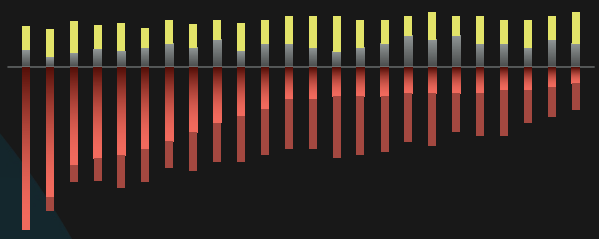


Java Findings with Veracode Fix Coverage



Flaws created faster than they are fixed

At Scale



Security debt decreases over time

1. Veracode State of Software Security Report 2023

Shift-left

Static Code Analysis & Veracode Fix

Developers can significantly improve their efficiency by shifting security left in the development cycle. Shifting security left in the implementation timeline means adopting Static Code Analysis to identify vulnerabilities as developers are writing code. By moving security activities to the left of the development timeline, organizations can identify and address potential security vulnerabilities and risks at an earlier stage, ultimately reducing the likelihood of costly and time-consuming issues down the line.

Static Application Security Testing ("SAST") is a security testing technique that analyzes source code or compiled binaries without executing them. It helps identify potential vulnerabilities, security weaknesses, and coding errors by examining the code's structure, syntax, and logic. SAST scans the application's source code, libraries, and dependencies to detect issues such as buffer overflows, SQL injection, cross-site scripting (XSS), and insecure coding practices. It provides developers with actionable insights and helps them identify security flaws early in the development process, allowing for prompt remediation and improved software security. SAST is an essential tool in ensuring the integrity and security of software applications.

Developers can significantly increase their efficiency by leveraging Static Application Security Testing (SAST) and Veracode Fix. Veracode Fix recommends security solutions for common vulnerabilities while developers are in the process of coding, thereby reducing the time required to address flaws.

This approach prevents the disruptive downstream implications of revisiting code when developers or teams have moved on, saving valuable time and effort.

In Conclusion

A vibrant future awaits

The introduction of Veracode Fix represents a pivotal moment in application security testing, thanks to the fusion of Veracode's experience and responsible adoption of AI technology. Developers and security teams now possess a powerful tool capable of significantly bolstering the security of their applications.

Together, let us embark on an exciting journey towards a future illuminated by the convergence of AI technology and Veracode's 17 years of expertise.

Veracode Fix not only saves precious time and valuable resources, but also ensures that applications are secured against vulnerabilities early in the development lifecycle. With Veracode Fix integrated naturally into the software development life cycle at developers' fingertips, organizations can proactively safeguard their software, accelerate the delivery of secure software, and embark on a path of continuous security improvement.

We have the power to shape a new era of application security testing, laying the foundation for a world where software development not only survives but thrives, and where organizations focus more on innovation than on security debt.

Author

Brian Roche
CPO, Veracode

VERACODE

Veracode is a leading AppSec partner for creating secure software, reducing the risk of security breach, and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of process automation, integrations, speed, and responsiveness, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities.

Learn more at www.veracode.com, on the Veracode blog and on Twitter.