VERACODE

WHITEPAPER

Static Application Security Testing

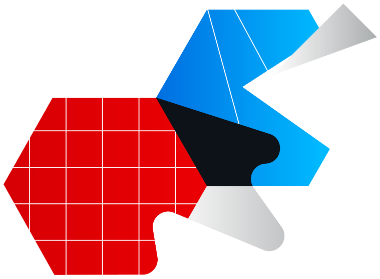
The Foundation of
Secure Applications

The Growing Security Challenge

Software vulnerabilities and cyberattacks are increasing in frequency and severity, posing significant risks to businesses. Exploitation of vulnerabilities surpassed phishing as the known initial access vectors in non-error, non-misuse breaches, according to the Verizon 2025 Data Breach Investigations Report.

The average cost of a data breach in 2024 reached $4.88 million

These vulnerabilities are compounded by the growing complexity of modern applications and the expanding attack surface. Vulnerability-based attacks skyrocketed by 124% in Q3 2024 compared to the same period in 2023[1], a stark indicator of the evolving threat landscape. So, what does this mean for your business? Financial losses and reputational damage. The average cost of a data breach in 2024 reached $4.88 million , a 10% increase from 2023.[2] And a successful cyberattack can severely damage your reputation, leading to a loss of customer confidence and market share. Securing your software is the cornerstone of mitigating such risks.



The Shift to Proactive Application Security from the Start

Given these alarming statistics, it is clear that a proactive approach from the beginning of the Software Development Life Cycle (SDLC) needs to be implemented. Traditionally, security has been reactive and has often been addressed late in the SDLC, typically during testing or after deployment. This reactive approach may lead to:

- **Increased costs:** Identifying and fixing vulnerabilities late in the SDLC is significantly more expensive and time-consuming than addressing them earlier.
- **Development delays:** Security issues discovered late in the process can lead to costly rework and project delays, hindering time-to-market.

To mitigate these challenges, organizations are increasingly adopting a proactive approach known as "***shifting left***." Shifting left involves integrating application security activities earlier in the SDLC, ideally starting from the initial design and coding phases. By doing so, organizations can identify and address security weaknesses when they are easier and less costly to fix, reducing overall risk and improving software quality. Integrating Static Application Security Testing (SAST) early in the SDLC is crucial to achieve this proactive security approach.

Understanding Static Application Security Testing (SAST)

Static Application Security Testing (SAST) is a methodology used to identify security flaws in an application's source code before it is deployed. Unlike Dynamic Application Security Testing (DAST), which analyzes applications during runtime, SAST examines the code itself to detect potential security weaknesses.

Here's how SAST works:

- **Static analysis:** SAST tools analyze the application's static code to identify patterns and code constructs that are known to be associated with security weaknesses.
- **Early detection:** By analyzing the code early in the development process, SAST enables developers to identify and fix flaws before they can be exploited.
- **Vulnerability identification:** SAST can detect a wide range of common security flaws, such as buffer overflows, SQL injection, and cross-site scripting (XSS) vulnerabilities.

The core benefit of SAST is early detection. By finding and fixing security flaws early, organizations can:

- Reduce costs and damage from exploits.
- Shorten development cycles.
- Improve the overall security posture of their applications.

Veracode Static Application Security Testing

Balancing Speed and Security across DevSecOps

In the realm of application security, the conversation has often centered on "shifting left" – the practice of moving security testing earlier in the development lifecycle. While the principle of early security integration is crucial, ideally the best approach to “shift left” is to provide support to prevent flaws from ever being written into code. Veracode’s approach extends beyond this singular focus. As highlighted in discussions surrounding "***shift-left pushback***”[3] and "***security soul-searching,***”[4]. Veracode emphasizes that true efficacy in DevSecOps isn't just about when security is shifted left, but how comprehensively and rapidly it's integrated from the very inception of code. This distinctive perspective highlights the need to secure code quickly from the start while ensuring comprehensive security coverage across DevSecOps.

Bridging the Gap Between Dev and Security

Veracode recognizes that developers are under immense pressure to deliver software rapidly, and security teams are tasked with ensuring that software is secure. Some SAST solutions offer a fragmented approach which results in security teams compromising quality for rapid "shift-left" findings; this pursuit of speed often conflicts with accuracy, leading to a proliferation of false positives that ultimately negate the intended benefits by consuming valuable time and resources. Traditional SAST forces a choice between being overwhelmed by false positives or missing critical vulnerabilities. Veracode stands apart by providing a balanced solution that addresses the needs of both development and security — ***comprehensive coverage and accuracy*** — fostering collaboration rather than conflict.

Comprehensive Coverage Without Compromise

Veracode provides an approach that delivers speed with comprehensive coverage without compromising quality, which is often a tradeoff with other vendor solutions. Veracode is pushing the boundaries of SAST technology to give developers and security teams the best of both worlds. Veracode's unique value proposition lies in its ability to provide findings quickly, with the comprehensive coverage that organizations need.

You should not have to choose speed over accuracy. Instead of customers adapting to how a tool works, Veracode's configurable SAST scanner adapts to developer and security team use cases, seamlessly integrating with your DevSecOps workflows to ensure your tools work the way you need them to, delivering superior results. **Veracode SAST** prioritizes the accuracy and comprehensiveness of scan results. While source code analysis offers early feedback and seamless DevOps integration, and binary analysis provides post-build completeness and third-party coverage, you shouldn't have to choose between their strengths. This is where Veracode delivers, ensuring comprehensive coverage by uniquely combining the benefits of both approaches.

Speed Without Accuracy

The challenge developers face is speed without accuracy. The problem isn't with security scanning itself, it's with forcing an impossible choice between speed and accuracy. However, this pursuit of speed results in a high volume of false positives. These inaccuracies are detrimental to developers, who waste valuable time chasing non-existent threats, and to security teams, who struggle with unreliable data and a jeopardized security posture. High false positive rates negate the very benefits of "shifting left," a significant emphasis in the SAST market, and lead to wasted resources burned without tangible security improvements. Developers often disable security scanners after spending hundreds of hours chasing false positives.

The Veracode False Positive Advantage

Veracode's comprehensive whole-program analysis, encompassing techniques like contextual guidance to prioritize efforts, enterprise-wide policy control, reporting, and analytics, advanced data and control flow modeling, inter-procedural scanning, and more, ensures a remarkably low false positive rate of less than 1.1%. This precision means developers can trust the results and focus on real threats, while security teams gain reliable insights for governance and compliance. Some of the capabilities that help keep false positive rates low:

> **Reachability and "taint tracing":** To ensure precise security findings, Veracode reports on reachable flaws — those programming constructs an attacker can execute, invoke, and control. This is achieved through sophisticated techniques such as dead code elimination, exclusion of code in comments, in-depth comprehension of data flow (how data propagates through the program) and control flow (the operational sequence of the program at runtime), and critically, tracing the flow of potentially tainted data via robust pointer analysis to determine if an attacker can deliver a malicious payload to the vulnerable code. This methodology represents a significantly more sophisticated approach than basic pattern matching or regular expression "grepping" for code patterns.

> **Full program analysis:** Examining smaller code segments, such as a single class or file, reduces scan time, but this approach significantly compromises accuracy, leading to a substantial increase in both false positives and false negatives. By limiting analysis to isolated components, crucial contextual information regarding runtime invocation, data flow, and control flow is lost, thereby preventing effective reachability analysis and the reliable determination of potential attack vectors. Veracode champions comprehensive full program analysis to overcome these limitations, supporting applications up to 5GB of code — a critical advantage for extensive legacy codebases or complex collections of microservices — ensuring thorough and accurate security insights.

> **Framework support:** A significant challenge in performing static analysis on modern applications stems from the reality that much of the control flow logic resides not within the application code itself, but within underlying frameworks. In contemporary web applications, frameworks typically implement standardized control flow patterns (e.g., Model-View-Controller), with the application code primarily providing instructions to these frameworks. Consequently, a static scanner lacking comprehensive framework understanding may misinterpret a single method call, a configuration entry, or an annotation, thereby failing to recognize unsafe framework invocations. To effectively address this, a static scanner must robustly support the framework's data and control flow, comprehend the functionality of its various methods and accurately model its behavior to evaluate customer code within its proper context. This profound understanding is precisely why Veracode's extensive support for hundreds of frameworks across all its supported languages is paramount for accurate and complete security analysis.

Veracode Framework Support

Veracode continually expands framework support by analyzing customers code to understand the relative importance of supporting new frameworks, which are added regularly.

Language	Frameworks
Java	63
.NET	33
JavaScript	22
Android	3 (plus Java and Kotlin frameworks)
Apex	3
Cross-Platform Mobile App Toolkits	7
Supported COBOL dialects and standards	17
Go	4
PHP	4
Python	9
Scala	3

Technical Deep Dive on SSCs

Consider a number being passed into a function that has no security consequences for receiving a negative value:

```
int main(void)
{
   unsigned int u = 0;
   u--;
   printf("%d\n", u);
   return 0;
}
```

Without the security sensitive context filtering, Veracode would report an integer overflow flaw; with the rule, this flaw is suppressed from the report. Veracode uses SSCs on a variety of numeric and memory allocation flaw categories.

Security-sensitive context filtering: In certain scenarios, particularly with vulnerability types concerning numeric size or behavior, identifying genuine flaws based solely on data and control flow analysis can be challenging. Often, specific security context factors indicate that a potential numeric anomaly is a coding error but carries no actual security implication. To address this, Veracode has implemented **Security-Sensitive Context (SSC)** rules. These rules meticulously review findings, suppressing those that arise in a security-irrelevant context and thereby leading to a dramatically reduced false positive rate for the scan.

Crosscheck: Given the inherent branching complexity and multifaceted nature of execution paths within a software application, an attacker may exploit numerous avenues to reach and compromise a flawed piece of code. Consequently, merely identifying a single path is insufficient to definitively establish a vulnerability; a comprehensive analysis of all potential attack vectors is imperative. Veracode's Crosscheck process directly addresses this critical requirement by exhaustively identifying and reporting every code path that could enable an attacker to reach vulnerable code via a patented process (US 9,286,063).

Continuous customer feedback loop: Every customer inquiry regarding static analysis results is meticulously reviewed and, when warranted, escalated to Veracode's dedicated engineering team for in-depth investigation. Resulting enhancements and fixes are rigorously validated against an expansive testbed comprising thousands of real-world and synthetic applications. Upon release, these improvements universally elevate scan accuracy for all customers. This iterative and continuous feedback mechanism is fundamental to how Veracode has engineered and maintains the industry's lowest false positive rate in the business. With thousands of organizations, from Fortune 500 enterprises to innovative startups, relying on Veracode's static analysis engine, this feedback loop has refined Veracode's accuracy across millions of scans and hundreds of trillions of lines of code.

Mitigating the False Negative Threat

While optimizing for a low false positive rate is crucial, an exclusive focus on this metric risks overlooking an equally, if not more, critical concern: the false negative. The judicious balance between suppressing noise and identifying genuine, critical vulnerabilities is paramount. Missing a significant finding can incur severe financial and reputational costs. This danger is most readily apparent in sectors such as critical infrastructure, healthcare, pharmaceuticals, automotive, or financial services, where a single undetected flaw in an automated system could jeopardize countless lives or result in multi-million-dollar losses. Every business must critically assess its own risk tolerance, weighing developer time against potential revenue impact. A security practitioner in the automotive industry starkly articulated the catastrophic potential of undetected vulnerabilities in a **2024 study: “False negative - that one is going to kill you.”**

This dynamic is vital when formulating an application risk strategy. The challenge for security and DevOps teams lies in the rarity of a single scanner capable of simultaneously delivering both a minimal false positive rate and comprehensive thoroughness.

Fortunately, many of the advanced technologies that enable Veracode's industry-leading low false positive rates also prove instrumental in mitigating false negatives. These include sophisticated data and control flow modeling, comprehensive full program analysis, robust framework support, and a continuous customer feedback loop. Rich framework support is particularly critical; as most modern software development frameworks govern essential functions like database access, display templating, APIs, and control flow. A deep understanding of these methods is indispensable for identifying instances where a software program misuses them, thereby introducing security issues.

However, achieving comprehensive false negative avoidance is computationally intensive. Proper interprocedural, data, and control flow modeling, along with full program analysis demand significant processing resources. Furthermore, an organization's "crown jewel" applications are often not nimble, well-architected microservices that scan and publish quickly; instead, they are frequently complex, monolithic systems that resist decomposition or retirement, inevitably resulting in lengthy scan times.

The Compromise of Speed

The market's emphasis on rapid scan times often prioritizes speed. While this appears, especially at first blush and for simple applications, to be advantageous, in the real world, it often comes at the cost of genuine security and accuracy, with any potential benefits wiped out by excessive false positives. This accelerated performance is often achieved by implementing technical shortcuts, such as relying solely on pattern matching instead of in-depth data flow analysis, conducting partial scans rather than comprehensive full program analysis, and neglecting critical framework context. When safeguarding production systems, the imperative shifts from a quick, potentially incomplete answer to a thorough, accurate security assessment.

Traditional Fast SAST	Veracode Deep Analysis
Pattern matching	**Full data flow analysis**
Partial/file scanning	**Complete program analysis**
Generic rules	**Framework-aware detection**
5-30% false positives	**1.1% false positives**
Misses complex bugs	**Catches sophisticated attacks**
Fast with less accuracy	**Thorough and accurate**

Veracode Fix: AI Code Remediation

Identifying security weaknesses is only half the battle; the true measure of an effective application security program lies in the ability to fix them efficiently. This is where **Veracode Fix**, an AI-driven tool, trained on proprietary data, helps to transform the remediation landscape.

Veracode Fix automates remediation guidance of vulnerabilities detected in your code, helping developers save time. It goes beyond merely identifying vulnerabilities by providing developers with targeted, actionable remediation advice and even applying fixes for identified vulnerabilities. This means developers can focus on building features rather than spending countless hours manually researching and fixing security flaws. For example, if a security flaw is found in a piece of code, Veracode Fix can suggest a fix right in a developer’s IDE and even apply it, upon user approval. This not only saves valuable developer time but also ensures that fixes are reliable and consistent as suggested fixes are curated by Veracode and not copied from unknown sources on the web, thanks to its responsible-by-design AI approach.

The impact of Veracode Fix across DevSecOps is profound

Accelerate Development Cycles: Developers using Fix see a 200% faster mean time to remediate (MTTR) compared to traditional methods[5].

Reduce Security Debt: Teams using Fix saw a 50% reduction in flaw density and 15x more flaws were remediated[6].

Automated Fix Suggestions that are accepted and implemented in 70% of cases, significantly reduce the time required to address vulnerabilities[7].

Pairs Well with Static Analysis: IDE plugins for Veracode SAST and Fix both led to a 92% reduction in time to detect flaws[8].

analysis, along with other analysis services in
Management Platform. The organization relie
external developers while also leveraging a la
components and libraries throughout the com
a pretty good job at actually monitoring our ex
vulnerabilities and remediating those vulnerab
according to our own policy." The organization
evaluate its security debt against that of its pe
Peer Benchmarking.

92%

Reduction in time to detect flaws compar

200%

Faster mean time to remediate security fl

INVESTMENT DRIVERS FOR VERACODE F

The AppSec leader at this insurance company
measured its developers' ability to find vulnera
and compared it to the legacy remediation au

The interviewee's organization adopted Verac
and the number of new flaws developed. They

- **Reliable and consistent recommenda** that Veracode Fix required less work to more accurate, and produced more pre

FORRESTER

Veracode Fix Improves Mean Time To Remediate Flaws By 200%

Veracode commissioned Forrester Consulting to interview four decision-makers and conduct a Total Economic Impact™ (TEI) study to better understand the benefits, costs, and risks associated with the Veracode Application Risk Management Platform.[1] This abstract will focus on a fifth interviewee with experience using Veracode Fix, a key value driver for the Veracode Platform.

Veracode Fix is an AI code remediation tool that helps organizations reduce security debt and eliminate new flaws. Along with Veracode Static Analysis, which automatically finds flaws, Veracode Fix integrates into common developer environments and workflows — integrated development environments, command line interfaces, and continuous integration/continuous delivery practices — to offer remediation tuned to an organization's specific requirements.

Forrester interviewed an application security (AppSec) leader at an insurance organization that tested and adopted Veracode Fix. Their company:

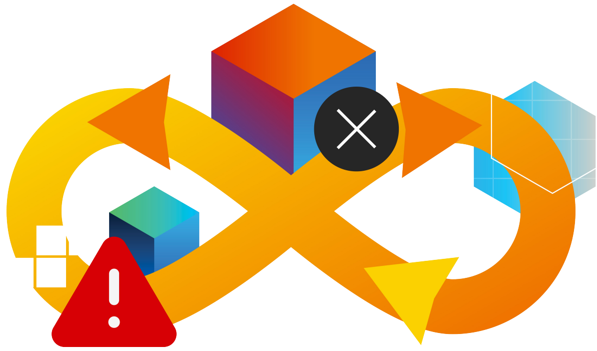
- Is headquartered in North America and has global operations.
- Employs between 5,000 and 10,000 FTEs with approximately 30 globally distributed security analysts and 6,000 developers, including outside contractors.

The interviewee's organization is beholden to various compliance authorities such as HIPAA and the Securities and Exchange Commission and has other reporting requirements. The interviewee noted, "We play by their rules for establishing an application security program and ensuring that we're managing risk according to that program."

The organization's application estate included 250 internal applications segmented from the company network and an additional 350 internet-facing applications that interact with customers and processed customer data. The interviewee noted that their organization relied predominantly on a custom code that it tested through static analysis and open-source software composition

To read the full report on Veracode Fix commissioned by Forrester, click here.

Veracode's Unified Find-and-Fix Workflow



The synergy between Veracode SAST and Veracode Fix creates a complete, continuous find and fix loop. Veracode SAST meticulously identifies security weaknesses across the entire application. Veracode Fix then steps in, providing the intelligence and automation necessary to resolve these issues at scale. This approach moves beyond traditional detection-only tools, delivering true remediation that accelerates releases, optimizes security workflows, and ensures safer applications with unmatched expertise.

Accelerating Secure Software Delivery with Veracode

Effective application security is not merely a safeguard but a competitive advantage. Veracode is continuously evolving its capabilities for DevSecOps, providing the most advanced scanning technologies for faster and safer scanning. Veracode is at the forefront of the SAST evolution, moving from scanning tools that retrospectively find flaws to intelligent software security solutions that proactively and automatically fix and prevent them. This means instilling software development tools with security-awareness, rapidly fixing security flaws, preventing insecure code from being written, and autonomously securing legacy code. Veracode's SAST approach empowers both developers and security teams to collaborate seamlessly, accelerating secure software delivery.

Veracode achieves this by providing a static scan service that is configurable, not a one-size-fits-all solution, to meet customers' specific use cases at each phase of the SDLC. This innovative approach ensures that security managers gain the accuracy they require, while developers benefit from the speed essential to their workflows, fostering collaboration without compromise. By providing a variety of scan configurations, Veracode will be able to provide results quickly with the ability to validate those results with more thorough scanning when required, distinguishing itself as the leader in driving secure software delivery. To learn more about how Veracode can transform your application security program and help you build safer applications faster, request a demo today.

Sources:

1 Vinugayathri Chinnasamy, "181 Key Cybersecurity Statistics: Vulnerabilities, Exploits, and Their Impact for 2025." Indusface, December 2024.

2. IBM, Cost of a Data Breach Report 2024.

3,4. Robert Lemos, Shift Left' Gets Pushback, Triggers Security Soul Searching, DarkReading. October 2024.

5, 6, 7, 8. Total Economic Impact Spotlight: Veracode Fix. A commissioned study conducted by Forrester Consulting on behalf of Veracode. April 2025.

VERACODE

Learn more at

www.veracode.com