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

analysis, along with other analysis services in the Veracode Application Risk Management Platform. The organization relied on some third-party code from external developers while also leveraging a large ecosystem of open-source components and libraries throughout the company. The interviewee said, “We do a pretty good job at actually monitoring our external applications for security vulnerabilities and remediating those vulnerabilities in very specific time periods according to our own policy.” The organization also worked with Veracode to evaluate its security debt against that of its peers using Veracode’s patented Peer Benchmarking.

> **92%**
>
> Reduction in time to detect flaws compared to manual processes

> **200%**
>
> Faster mean time to remediate security flaws

INVESTMENT DRIVERS FOR VERACODE FIX

The AppSec leader at this insurance company ran a proof of value exercise that measured its developers’ ability to find vulnerabilities manually without any tools and compared it to the legacy remediation automation tool and to Veracode Fix.

The interviewee’s organization adopted Veracode Fix to reduce its security debt and the number of new flaws developed. They noted investment drivers such as:

- **Reliable and consistent recommendations.** The interviewee indicated that Veracode Fix required less work to detect and remediate flaws, was more accurate, and produced more predictable results compared to

prompt-engineering-based conversational AI solutions. They further noted that using a conversational AI agent could vary widely in its recommendations based on which prompts were used: “[With prompt engineering solutions,] if you have two different people, they’re going to write a prompt differently. … You’re going to get different responses every time you ask it something. …That’s what we like about Fix. Its goal is to produce fixes with high confidence rates that will fix the security issue.”

- **Bespoke remediation steps.** The interviewee described how the tool’s AI/ML process tuned in conjunction with Veracode AppSec expertise and ensured a bespoke approach to their engagement. The interviewee described the power of frequent contact with Veracode application security coordinators (ASCs) in understanding the nature of different flaws, evaluating for false positives, and understanding the application code from a common weakness enumeration perspective. They shared: “[Veracode Fix is] using its own proprietary dataset to actually come up with a patch and its ASCs sit on calls to actually talk about flaws and have provided a lot of input into that model.”
- **Data privacy.** The interviewee indicated that data privacy was important to their organization’s selection of Veracode Fix as well as a differentiator in their market analysis. They said: “One really nice thing about Veracode is that it doesn’t use customer data in creating its own proprietary large language model for fixing code. We like that because our code is not going anywhere. We remain the intellectual property owners of that code.”

“We’ve all gotten used to prompt engineering … but this is a little bit different. With Veracode Fix’s AI machine learning models, you would always get a consistent analysis of the flaw and a code recommendation to fix that flow. [Compared with] any conversational generative AI or anything that uses a prompt, … Veracode is more curated with its patches and delivers them to you with a high probability of success.”

APPSEC LEADER, INSURANCE

KEY RESULTS FOR VERACODE FIX

The results of the investment for the interviewees' organization include the ability to:

Find flaws faster. Across all code types tested, including first- and third-party, the AppSec leader shared that their organization improved its time to detect security vulnerabilities in its code.

They also said that their organization saw a 92% reduction in the time to detect flaws with Veracode Static Analysis compared to their prior, manual AppSec processes: “It took [developers] roughly 150 minutes to find vulnerabilities with no plugin, and then that went down to 15 minutes with [our legacy tool that was not used much]. Then once we started to use Fix, it went from 150 minutes down to 12 minutes.”

Fix flaws faster. The interviewed AppSec leader remarked that their organization was able to remediate software vulnerabilities much faster than with its prior manual processes and decommissioned plugin.

They indicated a substantial improvement over their legacy software scanners in detecting and remediating flaws: “Not only is Veracode Fix tied into the new IDE, and static analysis is built right into the IDE, but it also gives us flaw remediation faster. You’ve got to wait literally less than 30 seconds, and you’ve got something that would take you hours to write. … The mean time to remediate versus our legacy [automated tool] was over 200% faster because we [started from] a very manual process.”

Fix more flaws. The interviewee discussed multiple ways in which Veracode Fix amplified their organization’s remediation efforts, including:

- **A higher fix rate.** Better remediation context made it easier for developers to fix flaws, which helped them fix more. The interviewed AppSec leader reported: “[We are] fixing flaws 17 times faster than manual efforts, which … resulted in a higher fix rate because of that contextual remediation guidance. Developers were able to read that, understand it, and see what changed to correct the security vulnerability. They also were very aware of the guardrails … and of not introducing any new vulnerabilities.”

- **The ability to batch process.** The interviewee said: “Now, you can do batch processing as well. And I think what happens is, once developers are successful or competent in using the UI for fixing vulnerabilities and they understand the different classes and categories of flaws, then they can process them as a batch. That's the real benefit of Fix, but only when you have the confidence in the recommendation to do that.”

Fix flaws better. The interviewee discussed how their organization improved important code quality metrics like flaw density per megabyte of code with Veracode Fix. Better context and faster processes compounded, making it easier for developers to fix more flaws and therefore produce and refine a higher quality code base. As a result, flaw density decreased by 50%, and 15 times more flaws were ultimately fixed. Veracode Fix helped to:

- **Develop higher quality code.** The interviewed AppSec leader said: “We measure our flaw density in our applications and that flaw density has probably gotten [cut] in half now. … [Regarding] the number of defects fixed, when it was a manual process, they only fixed about 4.5% to 5% of defects. Then when they used Fix, that went up to about 80%.”
- **Reduce security debt.** The interviewee said: “It’s gotten better, the product continues to improve, and we continue to reduce our security debt as well as eliminating new flaws because we’re pushing it to developers’ desktops and burning down some of the backlog of the old flaws that [they] have.”

Additional benefits. In addition to fulfilling its primary investment objectives of finding and fixing code more effectively and efficiently, the interviewee discussed additional benefits conferred by their organization’s use of Veracode Fix, including:

- **Shorter release cycles.** The interviewed AppSec leader said: “It’s giving you contextual guidance on what the flaw is and it’s also providing a fix or a patch, and so it’s shortened times for releasing to production. It’s definitely helped address a lot of the medium and high flaws so they’re not holding up production releases as well. … We saw a better detection rate. Fix was 15 times more adept at finding security vulnerabilities earlier in the software development lifecycle compared to legacy, [manual] efforts.”

- **Higher scores on developer satisfaction metrics.** The interviewee said that Veracode Fix scored highly on developer satisfaction surveys and motivated developers to address flaws, shortening cycle times while shipping higher quality and more secure code. About 60% of developers participating in a proof of value exercise POV accepted a full or partial recommendation from Veracode Fix, whereas developer adoption of other remediation tools was below 20%. They said: “It’s definitely improved our developer experience. … [It took] 12 minutes, and [most of] that was to scan the entire application. A lot of developers really love that. … It motivated them to get the application patch fixed.”
- **Higher report quality and decreased time to insight.** The interviewee said Veracode Fix helped with faster reporting and better analytics capabilities: “Analytics has improved as well. The burn down of our product backlog continues to decrease, [and] that’s something that we measure. It’s [also] helped us improve reporting to our board of directors [on] meeting our commitment to … reducing our flaw density and our counts of flaws in comparison to the last year.”

> **150 minutes to 12 minutes**
> Time to remediate a flaw manually versus with Veracode Fix

TOTAL ECONOMIC IMPACT ANALYSIS

For more information, download the full study: "The Total Economic Impact™ Of The Veracode Application Risk Management Platform," a commissioned study conducted by Forrester Consulting on behalf of Veracode, August 2024. Additionally, learn about the platform's application security posture management (ASPM) solution, Veracode Risk Manager.

STUDY FINDINGS

While the value story above is based on one interview and focused on Veracode Fix, Forrester interviewed four total representatives at organizations with experience using the Veracode Application Risk Management Platform and combined the results into a three-year financial analysis for a composite organization. Risk-adjusted present value (PV) quantified benefits for the composite organization include:

· A 75% reduction in the risk of a software-based attack with policy-driven, automated workflows to lower security debt and deliver more apps that pass security policies.

· An 80% improvement in developer productivity, resulting in 70,000 developer hours reallocated to innovative product development efforts.

· An 85% reduction in manual AppSec workflows thanks to automation, reallocating almost 25,000 hours of manual AppSec resource labor.

· A 20% increase in revenue from an accelerated, more secure, and more customer-focused software development lifecycle.

Return on investment (ROI)
184%

Net present value (NPV)
$4.60M

Disclosures
Readers should be aware of the following:

This study is commissioned by Veracode and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Veracode Fix.

Veracode reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Veracode provided the customer names for the interviews but did not participate in the interviews.

Appendix A: Endnotes

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.


FORRESTER®