How Veracode Can Improve Your Fix Rate

The most important function of an application security program is effectively fixing flaws once they're discovered. But the speed of that fix rate matters — the time it takes for attackers to come up with exploits for newly discovered vulnerabilities is measured in days, and sometimes hours. Which means that it's crucial to not only find and fix flaws in your code, but also to do so as fast as possible.

Our most recent *State of Software Security* report, based on our platform data, found that more than 70 percent of all flaws remain one month after discovery and nearly 55 percent remain three months after discovery. One in four high and very high severity flaws aren't addressed within 290 days of discovery.

How can you improve your fix rate? A recent Forrester TEI report found that by implementing DevSecOps practices, building stringent security controls, and integrating vulnerability testing into their CI/CD pipeline, Veracode customers were able to reduce mean time to remediation by 90 percent. Resolutions that previously took 2.5 hours on average were reduced to 15 minutes, helping developers reduce their time spent remediating flaws by 47 percent.

HERE ARE DETAILS ON HOW VERACODE CAN HELP IMPROVE YOUR FIX RATE →

Defining your policy with Veracode security program management

Improving your fix rate is critical, but the sheer volume of vulnerabilities present in most organizations' application portfolios makes it necessary for them to make daily tradeoffs between security, practicality, and speed. There are just too many vulnerabilities for organizations to tackle all at once, which means it requires smart prioritization to close the riskiest vulnerabilities first.

For example, it's important to look at exploitability ratings to specifically prioritize those vulnerabilities that are both high impact and easier to take advantage of. The fact is, a high severity flaw with a very high exploitability score introduces a lot more risk than a high severity flaw with a very low exploitability score. But our data reveals that organizations are more often prioritizing flaw severity over exploitability.

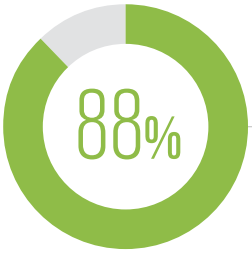
In addition, organizations should — in theory — be weighting the business criticality of an affected application into their prioritization calculations. When we looked at the data, however, we discovered that this isn't happening to a very large degree.

Veracode security program managers can work with you to help you better understand these priorities and to craft an application security policy that balances security, practicality, and speed to optimize your fix rate.

Addressing flaws with Veracode remediation coaching

Veracode helps developers fix what they find through contextualised remediation advice — a combination of high quality vulnerability descriptions and eLearning content supported by on-demand Application Security Consultant expertise.

Veracode application security consultants are all former developers who have extensive experience developing applications and working through challenging remediations.



We've found that our customers who take advantage of our remediation coaching improve their fix rate by 88% over those who don't.

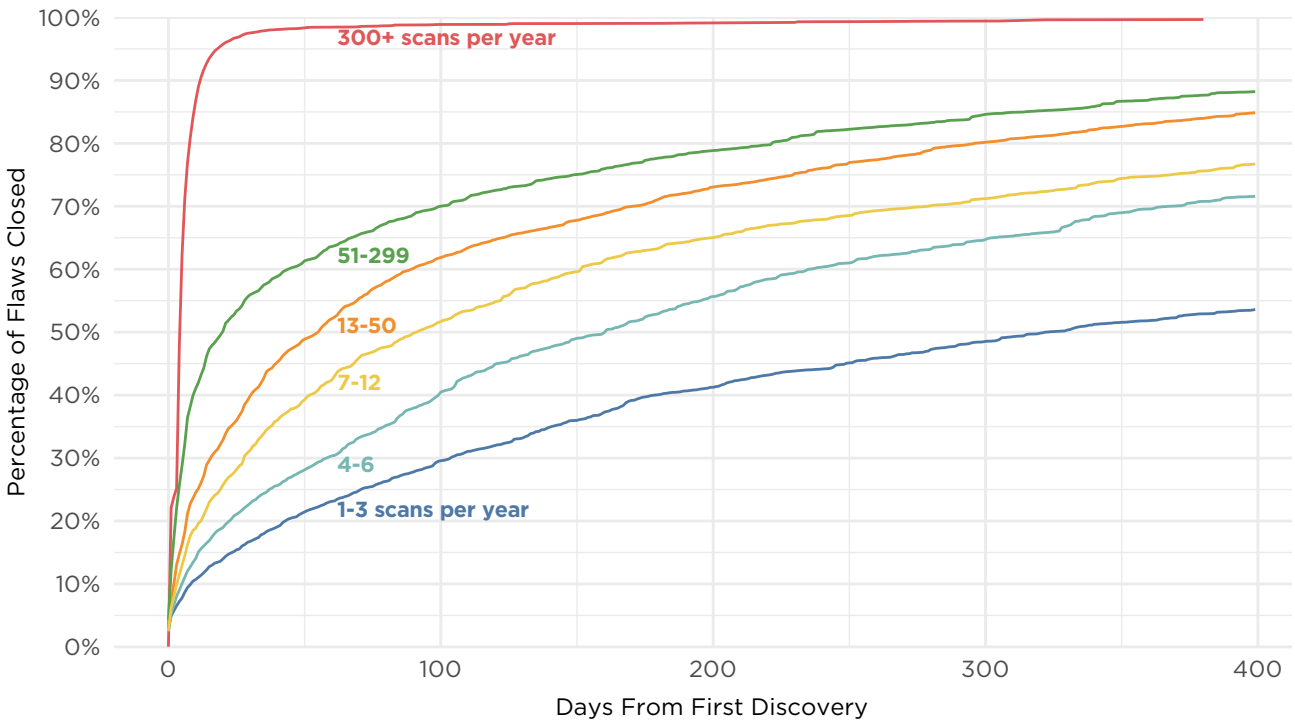
Scanning more

Simply put: Scan more, fix faster. Our data shows that there's a very strong correlation between how many times a year an organization scans and how quickly they address their vulnerabilities. In fact, every jump in annual scan rates sees a commensurate step up in the speed of flaw fixes.

We've found that flaws persist 3.5x longer in applications only scanned one to three times per year compared to ones tested seven to 12 times per year.

Once organizations are scanning more than 300 times per year, they're able to shorten flaw persistence 11.5x across the intervals compared to applications that are only scanned one to three times per year.

FIX VELOCITY BASED ON SCAN FREQUENCY



Source: Veracode SOSS Volume 9

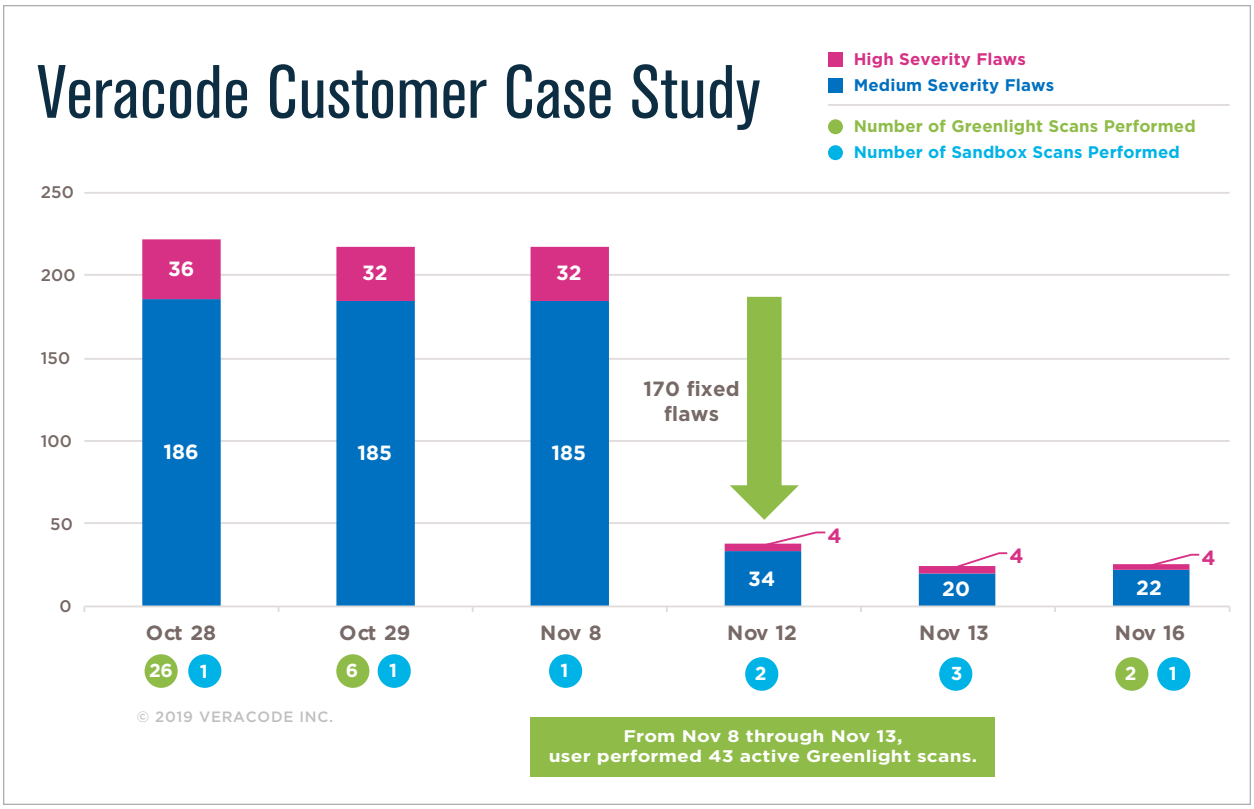
Avoiding flaws with Veracode Developer Training, Developer Sandbox, and Greenlight

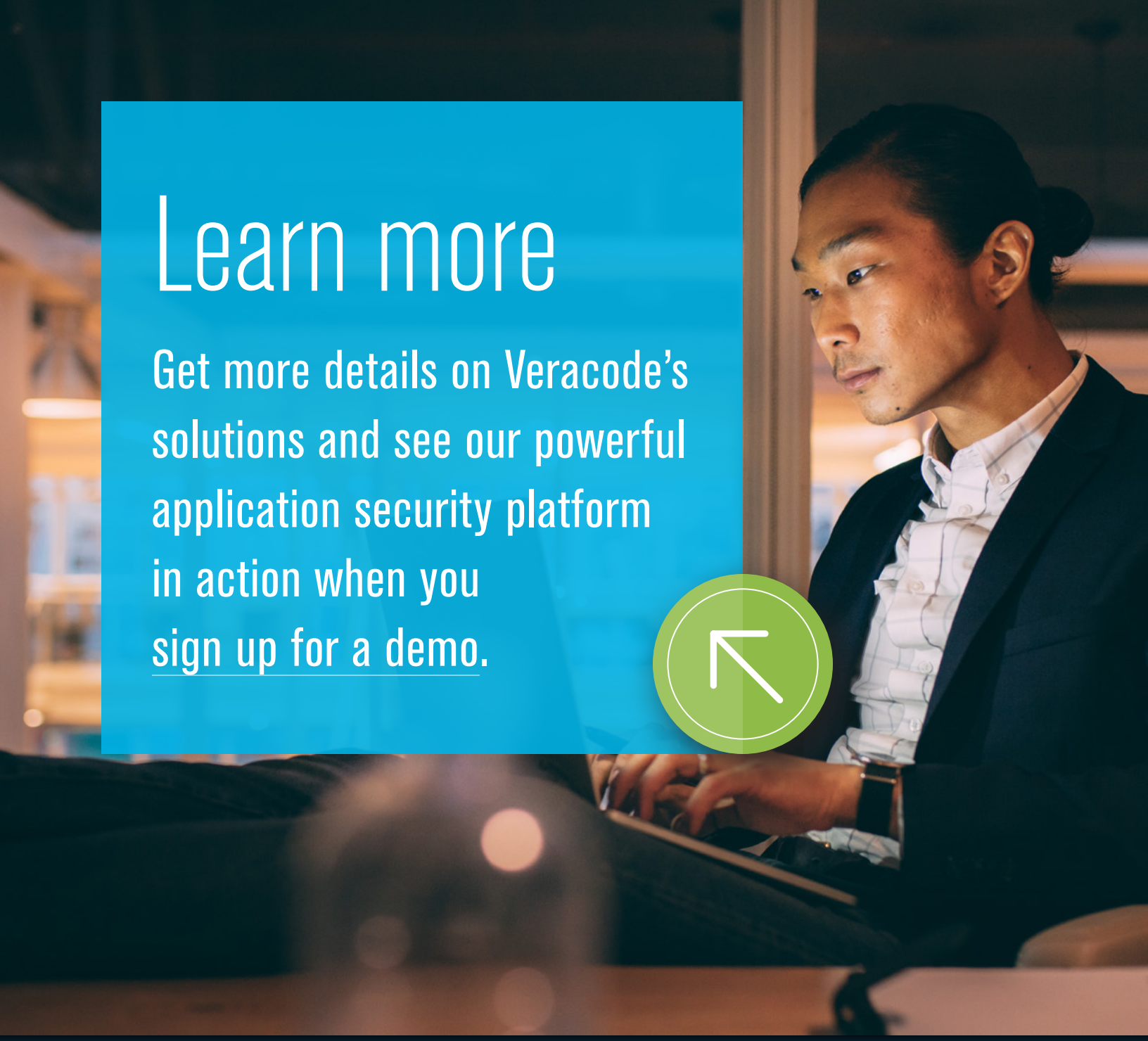
The fastest flaw to fix is the one that's never introduced into your code in the first place.

When your developers take advantage of Veracode Greenlight for in-line, incremental scanning; Developer Sandbox for early scanning without affecting the policy compliance of the overall application in production; and developer training on secure coding, they fix flaws earlier and faster. In addition, they learn to code more securely so they avoid introducing the same flaws in the future.

Our customers who take advantage of our developer eLearning on secure coding improve their fix rates by 19%.

See the chart below for a look at the fix rate improvements gained by one customer who is scanning code with Greenlight and Developer Sandbox.





Learn more

Get more details on Veracode's solutions and see our powerful application security platform in action when you sign up for a demo.

VERACODE

Veracode gives companies a comprehensive and accurate view of software security defects so they can create secure software, and ensure the software they are buying or downloading is free of vulnerabilities. As a result, companies using Veracode are free to boldly innovate, explore, discover, and change the world.

With its combination of automation, integrations, process, and speed, Veracode helps companies make security a seamless part of the development process. This allows them to both find and fix security defects so that they can use software to achieve their missions.

Veracode serves more than 2,000 customers worldwide across a wide range of industries. The Veracode Platform has assessed more than 8 trillion lines of code and helped companies fix more than 36 million security flaws.

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