Application Security

BEYOND SCANNING

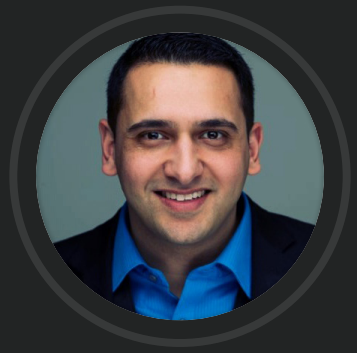
VERACODE

Everyone involved with application development will tell you that application security is essential. But not everyone agrees on how to go about securing their applications.

We consistently come across organizations that think they can check the AppSec box if they're scanning their code, or who are quantifying success by how many scans they can run a day, rather than by how many flaws they were able to fix.

Unfortunately, you can't scan your way to secure code. While the use of scanning tools in the CI/CD pipeline is incredibly valuable for identifying AppSec issues, the vulnerable code will go unaddressed by teams that don't have the knowledge, resources, or processes in place to address or mitigate the flaws they find.

To make AppSec truly effective at reducing the risk of a damaging breach, an organization must take three critical steps beyond scanning to develop more secure code: educating your developers so they learn secure coding skills, fixing the vulnerable code that's found, and scaling the AppSec program to cover your entire application landscape.



While I agree with the sentiment that security needs to be embedded in the build process, I am always surprised that a "tool integrated into a CI/CD pipeline" is as far as the planning typically goes.

— PEJMAN POURMOUSA, Vice President of Program Management, Veracode

Education

DO IT RIGHT THE FIRST TIME

While an AppSec strategy based on scanning can help you find flaws, a more effective approach is one that also aims to avoid flaws in the first place.

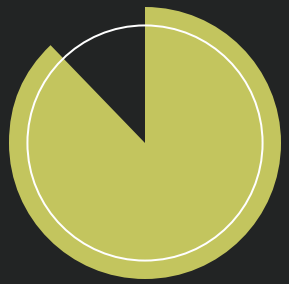
The fact of the matter is, too many developers lack the coding skills required to create secure code. According to our DevSecOps Global Skill Survey Report, nearly 70 percent of developers say their organizations don't provide adequate training in security. In addition, new employees aren't bringing secure coding skills to the table: 76 percent of developers who attended college say they weren't required to complete any security courses while in school. If developers aren't learning how to create code on the job or at school, where are they learning it? The answer: They aren't.

This lack of training and skills development keep many organizations from achieving their AppSec goals and objectives — such as meeting the compliance required by customers and regulators or reducing risk of breach. By helping developers understand security best practices, you can help them make your code secure from day one.

Nearly 70%
of developers say their organizations don't provide adequate training in security.

19%

Among our customer base, developers who use eLearning fix 19% more flaws than those who don't.



88%

Developers who get coaching from security experts fix 88% more flaws.

The time it takes to write secure code and insecure code is virtually the same, but creating secure code from the start can eliminate days of work finding and fixing bad code later in development or after a product has shipped. By shifting security left through preventative training, you can take the first major step to scaling AppSec.

Tailor your developer training based on the makeup and specific needs of your teams. For instance, eLearning can help developers learn when it's convenientor whenever they're faced with a specific challenge or vulnerability, while instructor-led training provides industry best practices along with product-specific issues.

In addition to training, you can use tools like Veracode Static Analysis, which help developers identify flaws in real time in their IDE. This not only allows developers to fix flaws while the issue is still fresh in their minds, but it helps them learn secure coding best practices as they code, reducing the overall number of flaws introduced over time.

By decreasing the number of security-related defects introduced in your code and providing tools to help quickly identify and fix issues, your teams can significantly reduce not only the number of errors that will be found in scanning, but also all the unplanned security work your developers would usually need to worry about down the road.

Fixing

GIVE YOUR SCAN A PLAN

Too many organizations put too much thought into finding flaws and not enough thought into what to do once they find them. Your teams can scan every single piece of code they write and run multiple scans a day, but without a plan in place to fix vulnerabilities, their code won't be much more secure than if they'd never run the scan at all.

The struggle to keep up with scan results is real. In our most recent State of Software Security report, we found that the mean time to remediation of software vulnerabilities is 171 days.

To effectively keep up with vulnerabilities, you should assess every scan against a policy that filters results by parameters you set for risk tolerance. This policy should also include guidance around how often your teams run a scan, how long they have to fix flaws based on severity or criticality, and which scanning techniques should be used.

Once you have a list of flaws, where do you start? Prioritization is key. The sheer volume of open flaws within an enterprise can be staggering. That means you need to be able to identify an effective way for determining which flaws to fix first and which can be left on the back burner. While many organizations do a good job prioritizing by flaw severity, make sure you also consider other risk factors.

For example, exploitability measures the likelihood of a flaw being attacked, rather than just its potential impact on the application, while application criticality tells which applications should receive the most attention. By using metrics beyond flaw severity, you can specifically prioritize those vulnerabilities that are not only high impact but that are likely to be taken advantage of or capable of causing outsized business disruption for your organization.

Once you've prioritized flaws, make sure your developers have the remediation guidance they need to fix specific security findings while learning to avoid similar issues going forward. Finally, remember that remediation takes time. Just scanning multiple times a day and logging vulnerabilities in a tracking system won't do any good if your teams don't have the bandwidth or schedule to make a fix. Rather than prioritizing multiple scans throughout the day, you're better off setting a more realistic scanning schedule — like once a day — while budgeting time for developers to fix what they find. You can always increase your scan frequency as your code becomes more secure and passes your policy on a regular basis.

Scaling

GIVING SECURITY SUPPORT

You've introduced training to reduce the number of flaws created while implementing a plan to prioritize fixes. Even then, chances are that your security team will still struggle to help all your development teams fix every last flaw their scans find, especially if you have one centralized security team tasked with helping multiple development teams. Any successful AppSec strategy needs to be one that can scale. These resources can help:

Expert help

Security champions

Cloud-based solution

Expert help

While development team training is important for educating developers about security best practices, it's unrealistic to expect all of your developers to become security experts. To overcome this skills shortage, outside AppSec expertise can be useful in helping to establish your security program's goals and roadmap. More importantly, it can help keep your roadmap on track by guiding developers through the fixing of flaws your scans find.

We've seen first-hand the difference this outside help makes. By augmenting security teams with our specialized AppSec expertise, Veracode customers who work with our Security Program Managers have been able to grow their application coverage by 25 percent each year. This helps these organizations decrease their time to deployment while improving vulnerability detection and remediation metrics. Our Security Program Managers do this by helping onboard security teams, ensuring security programs stay on track, and providing insights into new trends so programs continue to evolve along with security requirements.

Security champions

Another effective strategy is to develop and nurture security champions within your development teams. While these developers aren't (and don't have to be) security pros, they can act as the security conscience of the team by keeping their eyes and ears open for potential issues. The team can then fix the issues in development or call in your organization's security experts for guidance.

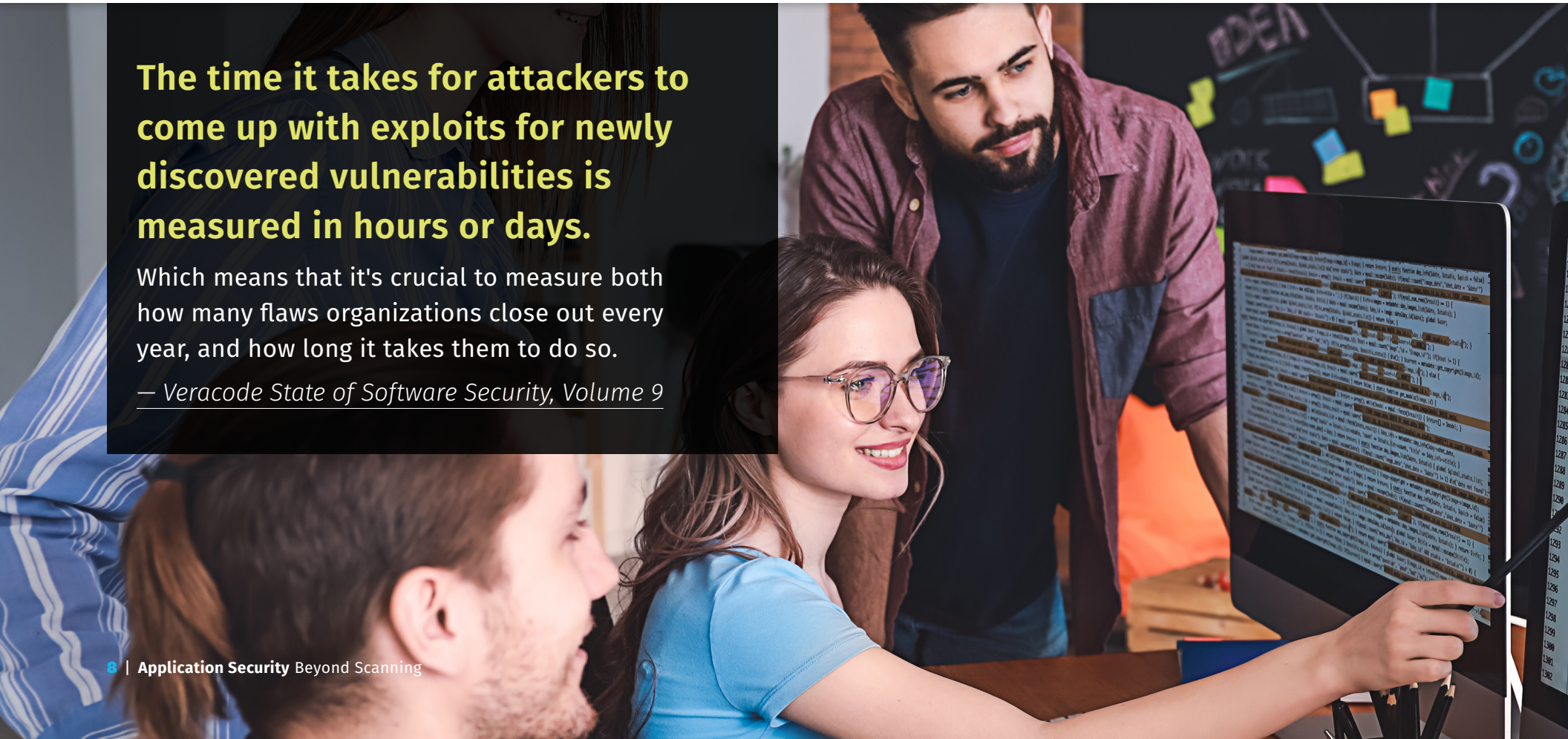
An embedded security champion can effectively help an organization make up for a lack of security coverage or skills by acting as a force multiplier who can pass on security best practices, answer questions, and raise security awareness. Because your security champion speaks the lingo of developers and is intimately involved in your organization's development projects, he or she can communicate security issues in a way that development teams will understand and embrace. By increasing the security quality of code at the development stage, you'll reduce bottlenecks at the security review stage and scale the amount of time available for your security team to work on high-value tasks.

Cloud-based solution

In addition, a cloud-based application security solution can help you scale your security without a lot of extra cost or hassle compared to an on-premises solution. Things that usually cost extra in an on-premises solution — features such as integrations, onboarding, upgrades, and maintenance — are all included with a cloud-based solution. This allows your security team to focus on scaling your AppSec efforts without worrying about going over budget.

A holistic approach to secure code

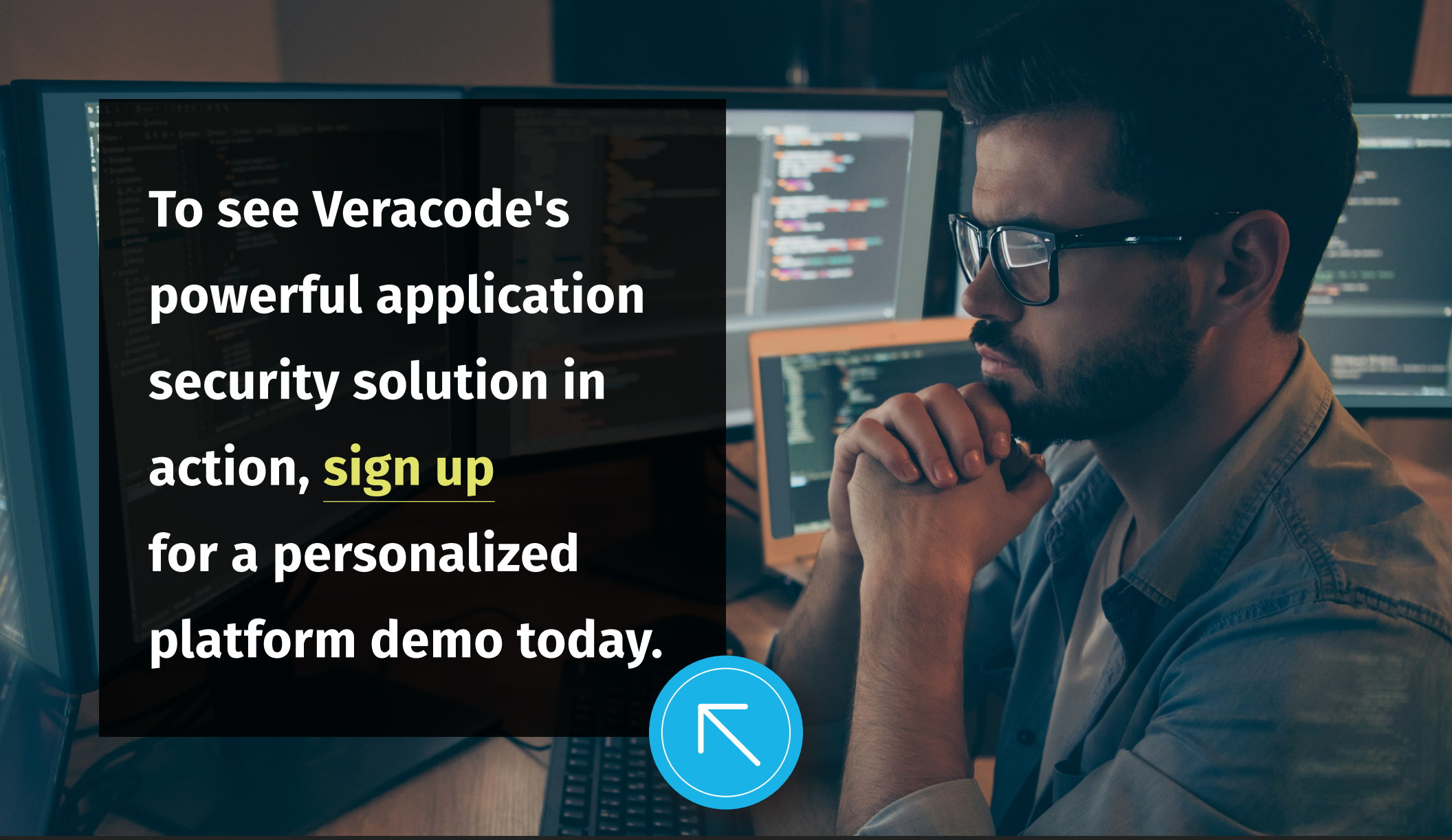
Without a doubt, scanning plays a critical part in ensuring that your organization creates secure code. But for true AppSec success, you must also have a strategy and tools in place to help your teams write secure code earlier in the process while fixing the flaws your testing does find. Veracode provides a suite of solutions and training to help you find, fix, and reduce vulnerabilities at scale. Learn more at Veracode.com.



The time it takes for attackers to come up with exploits for newly discovered vulnerabilities is measured in hours or days.

Which means that it's crucial to measure both how many flaws organizations close out every year, and how long it takes them to do so.

— Veracode State of Software Security, Volume 9



To see Veracode's powerful application security solution in action, sign up for a personalized platform demo today.

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.