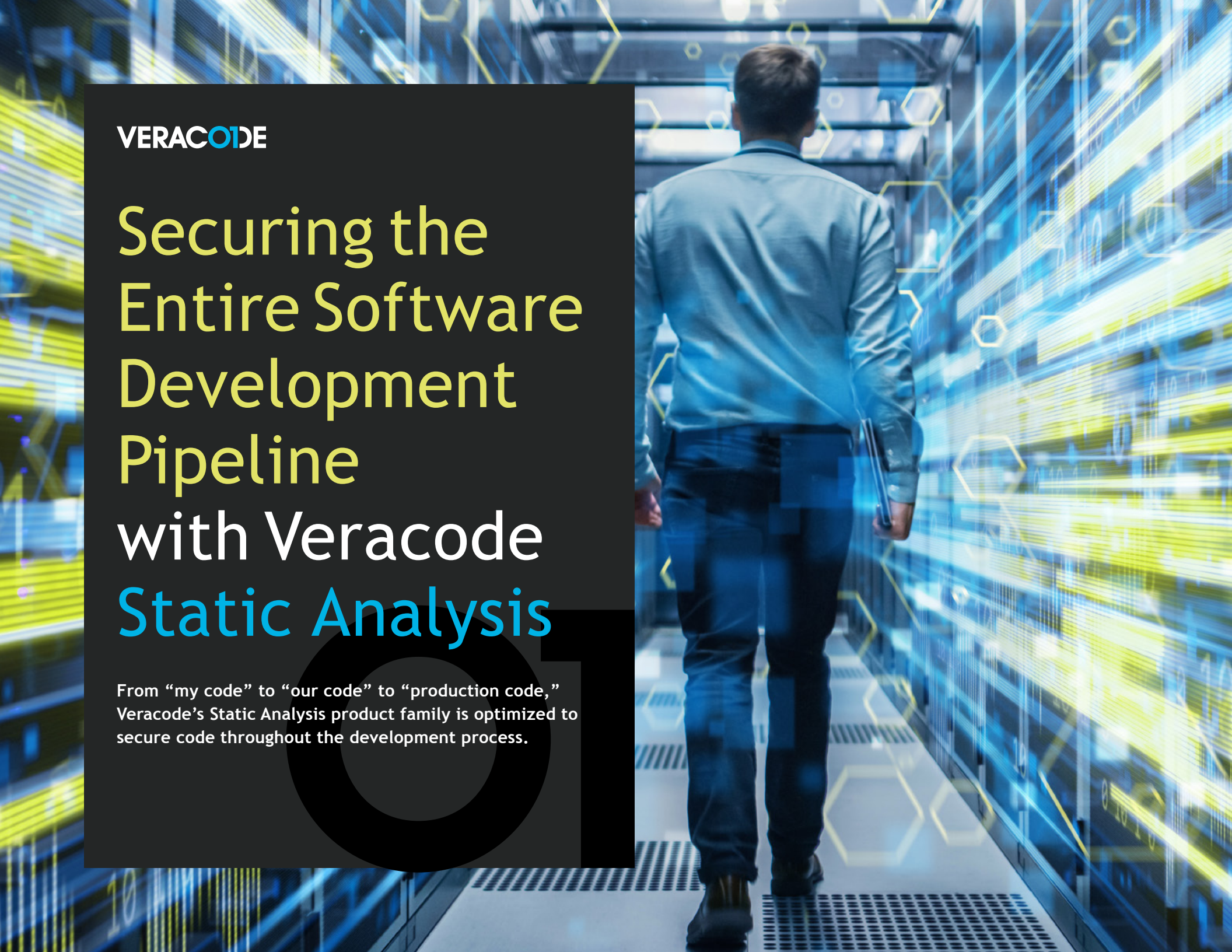


VERACODE

Securing the Entire Software Development Pipeline with Veracode Static Analysis

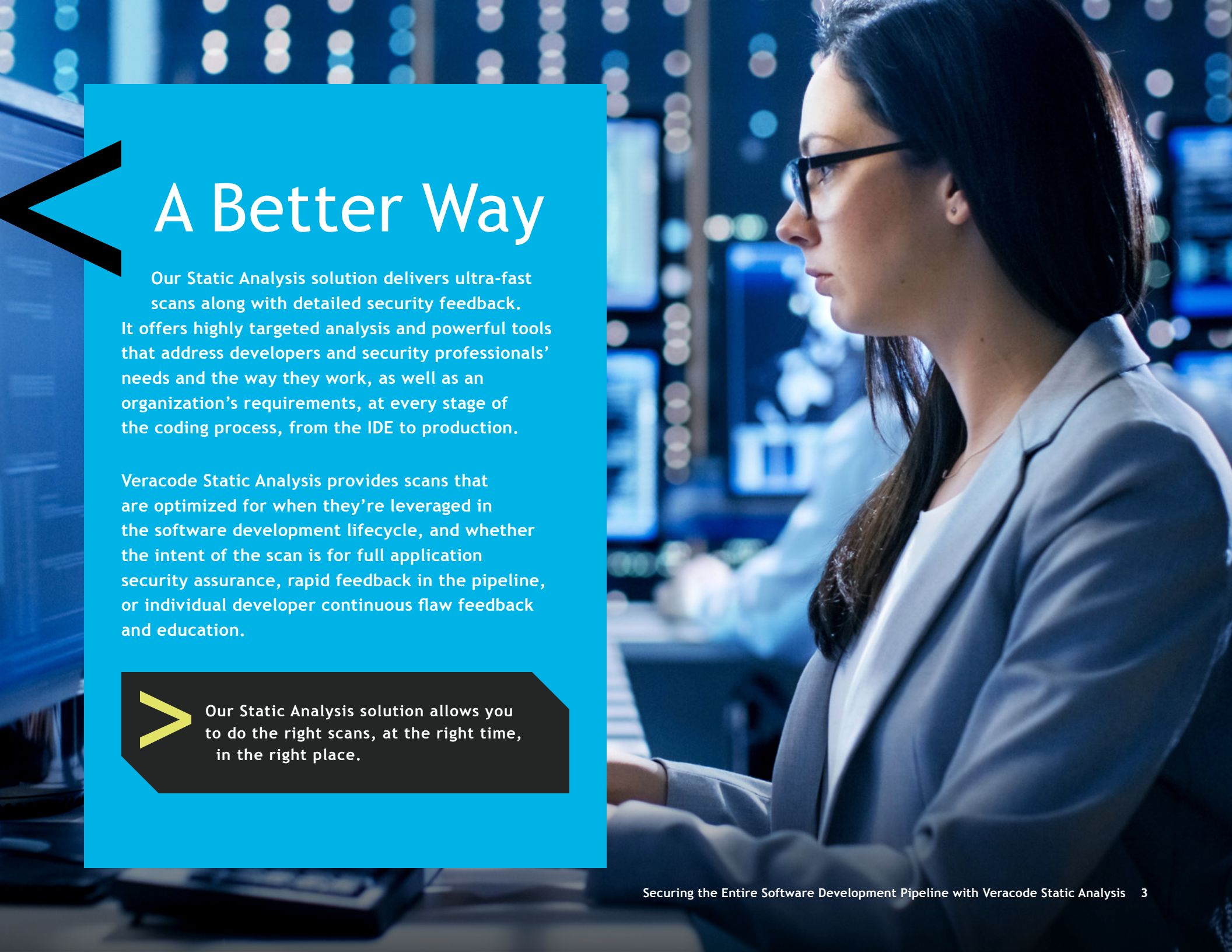
From “my code” to “our code” to “production code,” Veracode’s Static Analysis product family is optimized to secure code throughout the development process.

01

As organizations attempt to reduce the time it takes their development teams to create and release new software, development practices are rapidly changing. Modern development practices hinge on fast, agile processes with no roadblocks. And developers need security testing solutions that can keep pace.

But many traditional AppSec solutions — which focused solely on scanning completed applications against policy — created these roadblocks. Often taking hours to complete, these solutions left developers unable to move forward, provided feedback out of context, and delayed the release of software.

Veracode's Static Analysis solution works for organizations seeking to better secure their applications without reducing development velocity within the business. It's designed to deliver faster, automated security feedback earlier in the pipeline as well as full policy scans later in the development cycle prior to final code release. The result is unsurpassed accuracy and agility, and improved compliance with critical industry standards and regulations. Veracode Static Analysis delivers the right scan, at the right time, in the right place.



A Better Way

Our Static Analysis solution delivers ultra-fast scans along with detailed security feedback. It offers highly targeted analysis and powerful tools that address developers and security professionals' needs and the way they work, as well as an organization's requirements, at every stage of the coding process, from the IDE to production.

Veracode Static Analysis provides scans that are optimized for when they're leveraged in the software development lifecycle, and whether the intent of the scan is for full application security assurance, rapid feedback in the pipeline, or individual developer continuous flaw feedback and education.

> Our Static Analysis solution allows you to do the right scans, at the right time, in the right place.

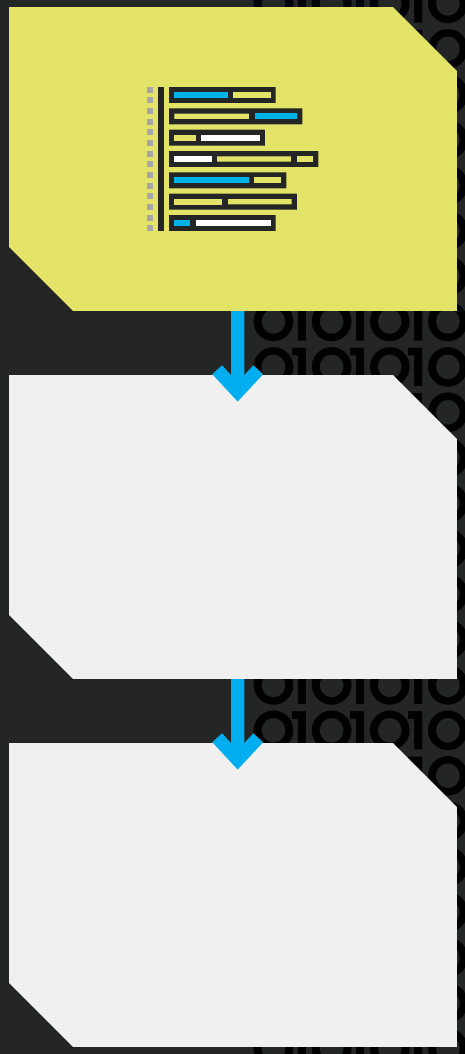
DEVELOPERS RATE THEIR DEVOPS PRACTICES AS

33% fair > 28% good > 17% poor

The most common reason cited for problems is manual processes/a lack of automation.[1]

Our updated Static Analysis solution addresses three primary areas of the development process with three different scanning types:

IDE Scan → Pipeline Scan → Policy Scan



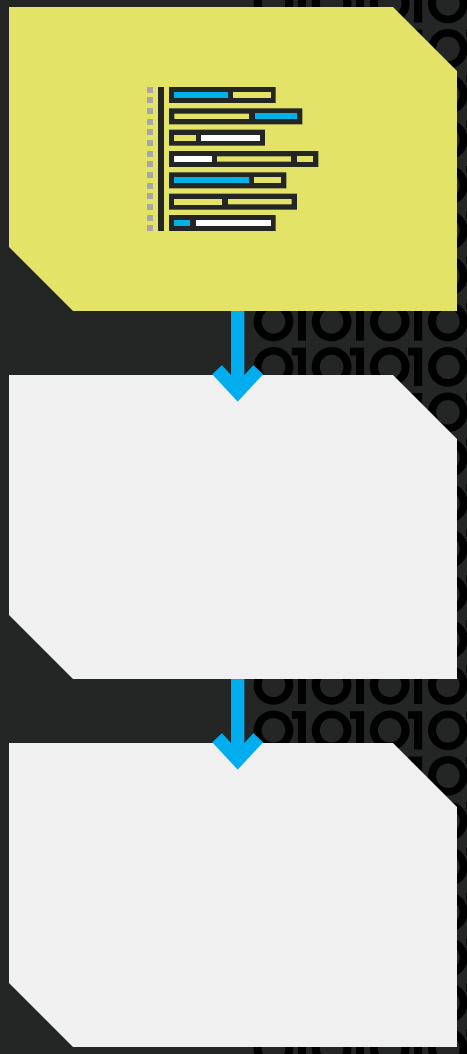
My Code

IDE / EDITOR (IDE SCAN)

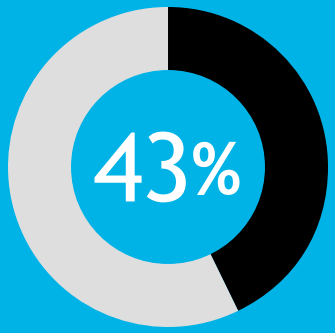
As developers write code, there's traditionally been no way for them to know if and when they're introducing errors and creating flaws. The IDE Scan analyzes the code that a developer is currently working on and provides real-time feedback to help developers answer the question "Is the code I'm writing secure?" before they commit it into the main repository.

BENEFITS

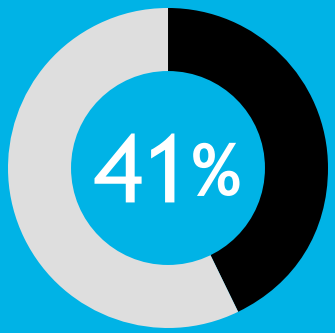
The IDE Scan provides feedback in seconds, reinforcing secure coding practices and flagging potential security flaws in real-time, which helps developers continuously build better secure coding practices. This approach helps reduce flaws introduced in new code by more than 60 percent on average. The IDE Scan also helps developers learn on the job through positive reinforcement, remediation guidance, code examples, and links to Veracode AppSec Tutorials.



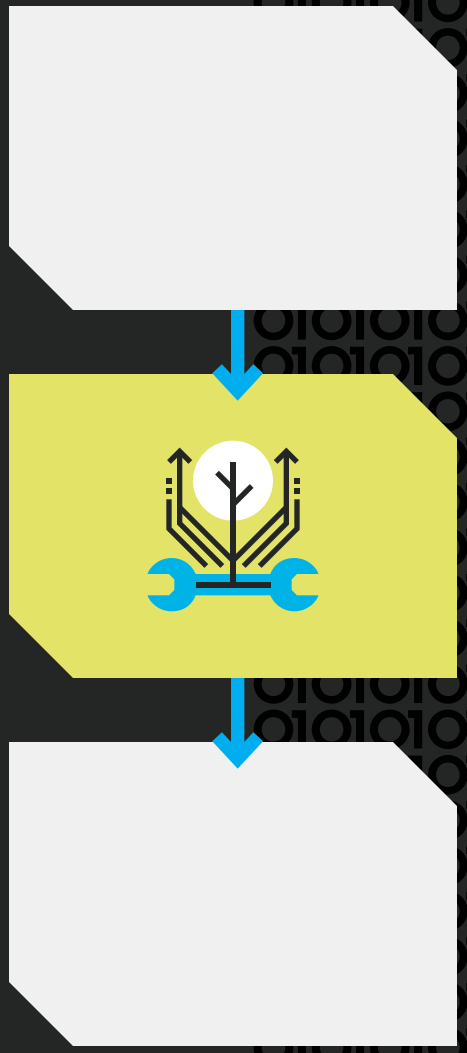
DEVELOPERS DEPLOY



multiple times a day



between once a day and once a month[2]



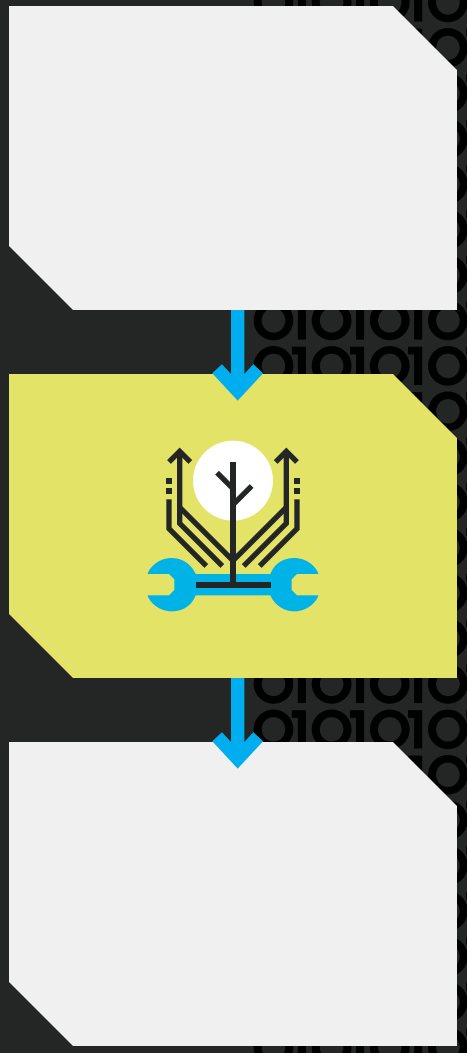
Our Code

CI PIPELINE (PIPELINE SCAN)

The Pipeline Scan integrates into the CI pipeline to offer test results each time code is committed. With a median scan time of just 90 seconds, this scan directly embeds into teams' CI tooling and provides fast feedback on flaws being introduced in new commits. It answers the question "Is the code my team is writing secure?"

BENEFITS

The Pipeline Scan is designed to run on every build to provide security feedback on the code at a team level on every commit. It offers crucial analysis and capabilities, including the ability to break the build if new security issues appear so that teams can prevent security flaws from entering their application and receive in-context feedback without triggering a full security audit.



There are currently more than

in public repositories.[3]

Production Code

CD PIPELINE (POLICY SCANS)

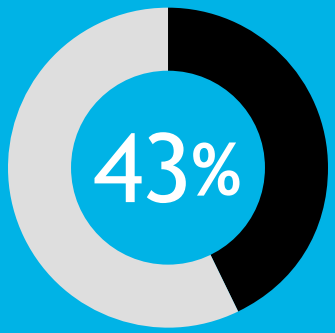
Ensuring that applications are meeting policy compliance and industry standards, the Policy Scan evaluates the entire application against one policy in a median time of eight minutes and delivers detailed analytics that can be used for any level of internal or external auditing. It can also notify a GRC system with the results of the scan. This scan answers the question "Are my organization's applications secure?"

BENEFITS

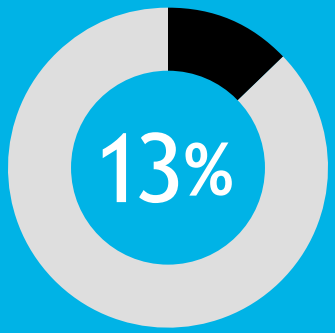
The Policy Scan generates reports that allow development teams to preview compliance in a sandbox before promoting the scan to policy and finalizing a release, update, or new software application. It produces the detailed information that auditors require and helps an organization achieve internal and external compliance. In addition, by providing visibility into how flaws are propagating over time at the developer, team, and business unit level, the Policy Scan's in-depth analytics allow security and development managers to proactively address risk across their organizations.

CONTINUOUS DELIVERY

— a cornerstone of DevOps — is a concept that developers view as critical.



believe that deployment must take place on-demand, which could include multiple deployments per day.



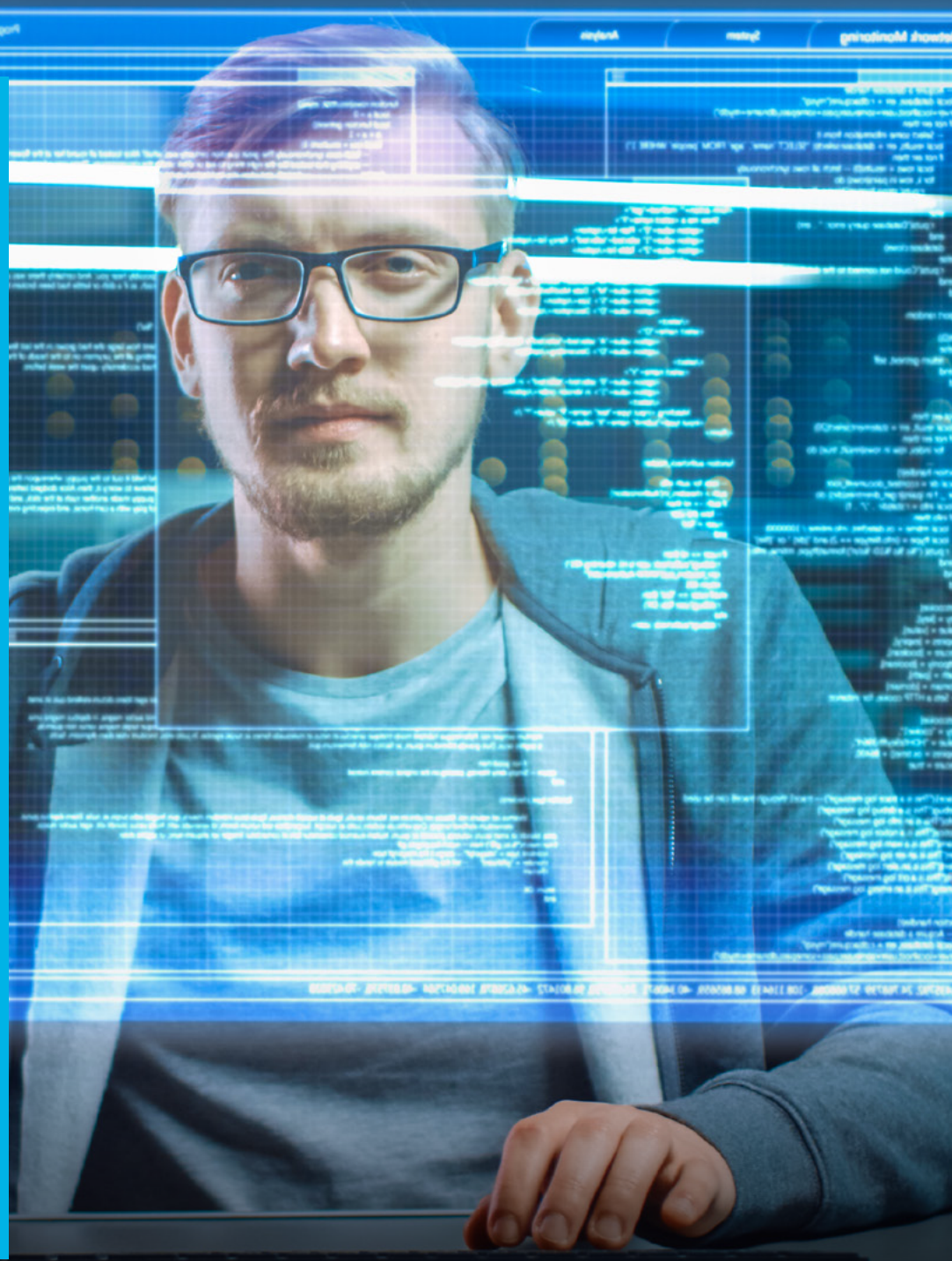
say that it's acceptable to deploy code between once a month and every six months.[4]

Scanning New Horizons

Our Static Analysis delivers a best-practice approach to static scanning. It makes accuracy a priority, producing a less than 1.1 percent false positive rate without tuning.

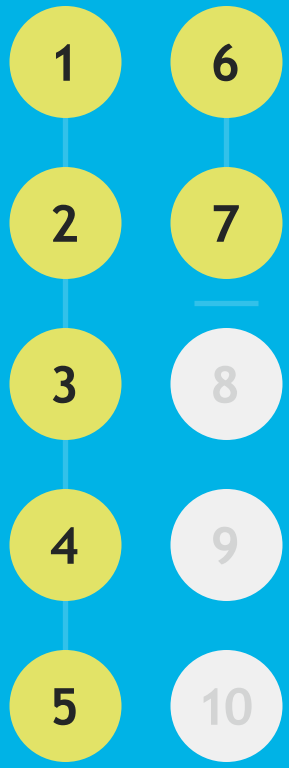
With this solution in place, developers are able to go about their work with a focus on security but without the burden of constantly stopping and starting for code reviews. They're also able to learn as they go through the use of constant feedback. Our Static Analysis provides quality results, including pointing out where flaws commonly take place, their severity, and the potential risk.

> By combining the IDE and Pipeline Scans, one major technology firm slashed the number of new flaws introduced into its master branch by 79 percent, compared to relying on policy scans alone.



DEVELOPERS SAY

70% ARE EXPECTED TO WRITE SECURE CODE



BUT RATE THEIR SECURITY PRACTICES AS ONLY

25% good

53% fair to poor[5]

To learn more

about our Static Analysis solution and how it can help you and your development team identify and remediate security flaws, please visit

OUR WEBSITE

[1] "2019 Global Developer Report: DevSecOps," GitLab.

[2] Ibid.

[3] "The State of the Octoverse," GitLab.

[4] "2019 Global Developer Report: DevSecOps," GitLab.

[5] Ibid.

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.