SYNOPSYS®

WHITE PAPER

Augment or Replace? How IAST Fits Into the AppSec Landscape

As the pace, volume, and complexity of application development continue to escalate, it becomes increasingly difficult to maintain the quality and security of software. More speed, more volume, and more complexity too often result in less quality and less security.

To ensure the proper balance, a time-honored issue must be addressed: bringing development, quality assurance (QA), and security teams into alignment. With alignment comes faster development that doesn't compromise quality or security. In order to achieve it, application security (AppSec) teams must meet their development peers where they are—in other words, they must build security into development test processes and workflows.

Empowering developers and testers to address quality and security inside their local development and test environments allows issues to be resolved quicker. It also enables security to keep up with the velocity and volume created by DevOps and agile methodologies.

How IAST can help

Interactive application security testing (IAST) is a revolutionary solution for organizations looking to balance the speed and complexity of their development with the quality and security of their applications.

Because IAST works concurrently with functional tests already running, it allows teams to do more at once and reduce security testing times. It's not an additional workflow or another tool or set of processes that developers need to manage and adopt, so it doesn't add any complexity. And by providing stack traces and remediation guidance, IAST gives development, QA, and security teams the contextual information they need to find and fix issues.

IAST gives development, QA, and security teams the contextual information they need to find and fix issues.

IAST adoption—the shift is on

IAST has been in the AppSec tool mix for several years. Not surprisingly, the majority of adoption occurs at the testing stage of the software development life cycle (SDLC). In a 2020 survey by Forrester, 40% of respondents were adopting IAST in the testing stage. Additionally, 38% were planning to adopt IAST in the development stage.[1]

"This is great news," said Sandy Carielli, principal security analyst at Forrester. "It [means] more organizations are working to build security in earlier in the process, and security issues are being addressed even earlier and aligned with functional testing."

When to augment and when to replace

When looking at the evolution of AppSec solutions within most organizations, there are many possible starting points: dynamic application security testing (DAST), penetration (pen) testing, static application security testing (SAST), or software composition analysis (SCA).

Tools such as SAST and SCA are great at finding vulnerabilities early in the SDLC, during code commit and iteration. But they can't anticipate vulnerabilities triggered during application runtime, compilation, and execution—especially in complex applications that are executed with open source and third-party components. IAST can augment SAST and SCA tools while bridging the gap between functional testing and security testing, further aligning development and security teams.

SAST and SCA tools find and fix security issues in code as it's being developed, and DAST and pen testing identify and report security issues in running applications. IAST combines these capabilities in applications and code during functional tests.

It's important to note that SAST and SCA are code scanners, so they add noise to developer workflows. False positives and duplicate findings are issues. IAST, on the other hand, isn't a scanner—it provides hybrid analysis.

No single tool can do it all. To ensure that applications are secure, organizations need a full suite of AppSec solutions that can test and detect vulnerabilities during static code development, component level integration, and at application runtime. However, IAST can serve as a replacement for missing tools or for tools not integrated well. For example, if your organization's existing DAST tool isn't well integrated into your software application workflow or CI/CD pipeline, IAST can be used instead because it can be integrated with functional testing tools and it aligns well with standard processes.

It's also important to keep your needs and goals in mind. No two organizations are the same. Your priorities may be to streamline or replace tools, or they may be to provide maximum coverage by augmenting what you currently have.

Seeker IAST—the Swiss Army knife in your AppSec toolkit

Many organizations struggle to automate their current workflows and CI/CD pipelines, and that creates a roadblock to implementing IAST. Synopsys' Seeker® is an industry-leading IAST tool that can help remove these limitations.

Thanks to its advanced instrumentation and patented verification technology, Seeker can be deployed quickly and easily with any of your functional test requirements. As long as your organization has test cases and some rigor in place around them, Seeker can be the "Swiss Army knife" to help in the various types of application testing your team performs—both ad hoc, manual unit testing and automated continuous testing.

It identifies, verifies, and pinpoints vulnerability and data leakage in your running applications and code without interfering with development processes and workflows. It can be a starter tool for manual functional tests because no security expertise is required. It has the agility to integrate security testing into existing functional testing, and it provides continuous verification and response, including failing the build automatically if critical security vulnerabilities are detected.

Looking ahead—or just getting started

To optimize (or begin) your AppSec program in general and IAST in particular, start testing earlier in the SDLC and expand testing expertise across your organization. This will federate testing excellence, allowing it to scale across the enterprise.

Automating key processes, such as code integration and delivery, as well as testing, design, execution, and orchestration will greatly expedite the software development process. If your organization is like most, your functional tests are 20% to 30% automated.[2] For more advanced teams using agile or DevOps methodologies, your functional tests may be closer to 50% automated.[3] And some mature adopters automate as much as 80% of their testing.[4] Wherever your organization is on this journey—if you've just started out automating your functional tests or you are fully mature—IAST can be instrumented to your apps and will perform dynamic runtime security testing in the background on its own.

At the same time, don't neglect the human element. Groom your full-stack developers and federate your testing center of excellence. This not only makes adopting IAST and other security tools easier, it effectively allows you to "shift left" and address security earlier in the SDLC, saving time and cost.

Ready to get started?

See how Seeker can help your organization maintain velocity while maximizing security

References:

[1] Forrester Analytics, Business Technographics Global Security Survey, 2020.
[2] Ibid.
[3] Ibid.
[4] Ibid.

SYNOPSYS®

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com