



GUIDE

Interactive Application Security Testing: A Buyer's Guide

Web applications continue to be the attack surface of choice for hackers attempting to access sensitive data. Per the “2020 Data Breach Investigations Report” from Verizon, successful attacks on web applications accounted for nearly half of all data breaches (43%), representing the single greatest cause of such breaches, and more than double the rate of the previous year.¹

Organizations clearly need to secure their web applications before they are deployed in production. But while development and application security (AppSec) teams often use static application security testing (SAST) and software composition analysis (SCA) solutions to identify security weaknesses and vulnerabilities in proprietary and open source code, they do so statically, at the code or component level. Many vulnerabilities can only be detected by dynamically testing an application during runtime test and release phases.

That’s why many organizations use dynamic application security testing (DAST) or penetration testing. DAST and penetration testing tools are run during QA or a late stage of production to detect vulnerabilities that can’t be found using SAST or SCA tools.

Additionally, while DAST and penetration testing can identify security vulnerabilities, they can’t pinpoint the lines of code containing the vulnerabilities. As a result, critical security issues identified by DAST can be problematic to fix and take a long time to resolve, putting remediation out of reach for the average developer.

Interactive application security testing

These challenges have led development and security teams to seek out alternative dynamic AppSec testing solutions such as interactive application security testing (IAST). IAST tools perform dynamic security tests concurrently during various test stages, while teams perform usual development and QA tests.

IAST tools can integrate seamlessly with continuous integration (CI) and test automation tools, as well as with agile and ad hoc test methodologies, and quickly generate analysis results that identify the specific lines of code where vulnerabilities reside. As a result, developers can fix issues quickly and push their commits as part of CI/CD or automation workflows.

More advanced IAST tools also incorporate SCA to uncover vulnerable third-party and open source components in an application.

Key benefits of IAST solutions

Actionable findings for development teams

IAST has been shown to reduce the time needed to remediate security vulnerabilities by 65% compared to penetration testing.² The reason for this is clear: IAST empowers developers to find and fix vulnerabilities as a part of the development process. Application security experts can remove themselves from the critical path of software development and spend more time on strategic security initiatives.

¹ Verizon, “2020 Data Breach Investigations Report,” <https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>.

² Forrester, “[Construct a Business Case for Interactive Application Security Testing](#),” Amy DeMartine, November 3, 2017.

Comprehensive vulnerability and security risk reporting earlier in the SDLC

IAST enables developers to fix security vulnerabilities as they test. This means finding and fixing runtime vulnerabilities in web apps before deploying them to production. “Shifting left”—doing security testing earlier in the integrated build and testing stages—shortens test cycles and enables substantial cost and resource savings while also reducing security risk.

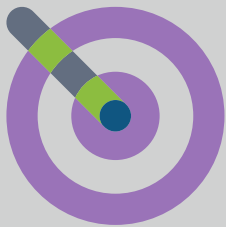
Low false-positive rates

IAST solutions automatically verify the results, ensuring a high degree of accuracy. They don't return a high number of false positives that require lengthy manual reviews, troubleshooting, and additional scans to resolve. IAST allows organizations to focus their security resources on more difficult corner-case vulnerabilities that require specialized expertise to identify and verify.

Seamless integration into automated development and testing environments

IAST solutions integrate seamlessly into CI/CD pipelines and run at the speed demanded by agile and DevOps. Both security and development teams benefit from integrating IAST into the SDLC—especially an IAST tool that provides SCA insights into vulnerable components, and contextual e-learning to help developers learn security on the job.

AT A GLANCE: Benefits of IAST



- Security testing “shifting left” in the SDLC
- Accurate results for fast triage (low false-positive rates)
- Pinpointing the source of vulnerabilities
- Seamless integration into current SDLC, agile, and CI/CD pipeline
- Earlier remediation at less cost and time

What to look for in IAST tools

There are many factors to consider when selecting IAST tools—and a handful of vendors to choose from. No matter which IAST solution your organization chooses, there are several minimum requirements to look for.

Updated security dashboards for standards compliance

Whether you're beholden to PCI DSS, OWASP Top 10, GDPR, SANS/CWE, or other sets of compliance standards, your organization needs insight into security risks, trends, and coverage—as well as security compliance for running web applications and services, including proprietary code and open source components.

Fast, accurate, and comprehensive results—out of the box

Low false-positive rates mean you spend less time finding and remediating vulnerabilities. Your IAST tool should offer out-of-the-box functionality so you don't waste time configuring and tuning tools to meet your requirements.

Real-time identification and reporting of vulnerabilities

Your IAST solution should automatically verify detect vulnerabilities and instantly prioritize vulnerabilities by severity levels so developers and AppSec teams can focus their time and resources on critical vulnerabilities that matter most to them.

Sensitive-data tracking

Organizations that need to achieve compliance with key industry security standards such as PCI DSS or GDPR need an IAST tool that lets them define the type of sensitive data they wish to automatically track and secure in their apps.

Ease of deployment in existing SDLC, agile, and DevOps workflows

Web application and DevOps teams rely on agile development and automation. Choose application security tools that seamlessly integrate with standard CI, test, and QA tools.

Enterprise-grade SCA binary analysis integration

Open source and third-party components, libraries, and frameworks are increasingly prevalent in web applications. Your IAST tool must provide visibility into open source security vulnerabilities and license types, as well as assurance that you're compliant with license requirements.

Detailed security guidance and remediation advice

An IAST solution should provide developers with detailed and contextual information about vulnerabilities, where they are located in their code, and how to remediate them.

Optimal support for modern technologies





More and more organizations are using APIs, microservices and serverless architecture to achieve speed of business innovation. An IAST tool should help teams detect and trace data flows and any tainted data used.

Questions to ask a potential IAST solution provider

- Are there any restrictions on the number of applications you can run the tool on?
- What is the license cost?
- What reputation does the vendor have in the AppSec space?
- What expertise or resources can the vendor provide to support developers and for general tech support?
- What programming languages and frameworks does the IAST tool support?
- How well does the IAST tool integrate with third-party tools?
- Does the IAST tool provide real-time verification and prioritization of detected findings?
- Does the IAST tool provide real-time, continuous feedback with line-of-code insights for timely remediation by development, security, or DevOps teams?
- Does the IAST tool support testing of web-based, cloud-based, and microservices apps?
- Does the IAST tool provide the contextual e-learning that your teams require?
- What regulations and compliance standards does the IAST tool support?

Black Duck® Seeker: The industry-leading IAST solution

Seeker® is Black Duck's award-winning IAST tool that helps development, QA, DevOps, and security teams automate security testing of modern applications (web-based, cloud-based, microservices-based, etc.). It's the industry's first IAST solution with patented active verification and sensitive-data tracking capabilities. It's accurate, easy to use, and scales to support enterprise needs while identifying and verifying vulnerabilities in real time. And where other IAST solutions stop at detecting and reporting, Seeker goes a step further by automatically verifying and prioritizing findings. It instantly reports vulnerabilities that matter to your organization.

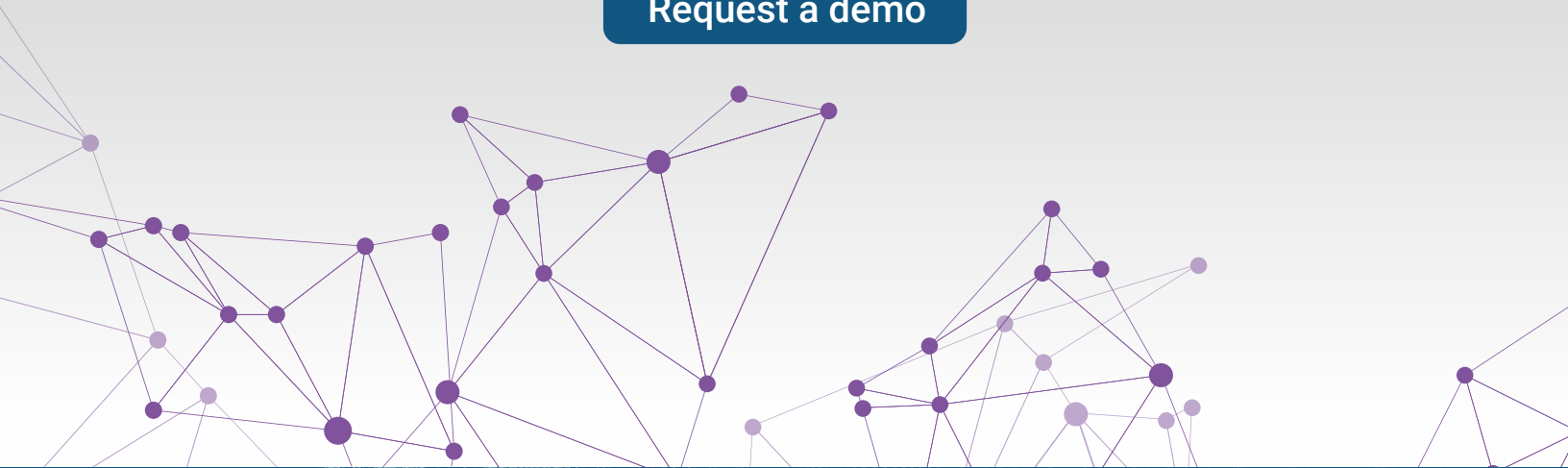
Integrated	Automated	Accurate	Actionable
 <p>Integrates with CI/CD workflows</p> <p>Extensive set of web APIs and out-of-the-box integration with Jira, Jenkins, Slack, and more</p>	 <p>Security testing automatically performed during functional tests</p> <p>Highly scalable and easily deployed</p>	 <p>Highly accurate—identifies the most severe vulnerabilities</p> <p>Patented verification engine + microservices and sensitive-data tracking</p>	 <p>Gives developers specific remediation guidance</p> <p>Traces vulnerability down to line of code</p>

Regardless of your organization's application test and security maturity, Seeker can benefit you.

- It's the ideal starter tool that will grow with an organization's testing needs
- It helps find vulnerabilities during manual and/or functional tests, reducing the need for additional security tests and scan cycles
- It integrates into the CI/CD pipeline and can automatically fail the build if critical security vulnerabilities are detected

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

[Request a demo](#)



About Black Duck

Black Duck[®] offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.