

LANDSCAPE REPORT

The Static Application Security Testing Landscape, Q2 2023

Forrester's Overview Of 22 Vendors

June 5, 2023

By Janet Worthington with Amy DeMartine, Danielle Chittem, Caroline Provost, Shayna Neuburg

FORRESTER®

Summary

You can use static application security testing (SAST) to reduce the time to fix application security weaknesses, improve application delivery speed and predictability, and prevent new weaknesses with fast feedback loops and secure coding education. But to realize these benefits, you'll first have to select from a diverse set of vendors that vary by size, type of offering, geography, and use case differentiation. Security and development pros should use this report to understand the value they can expect from a SAST vendor, learn how vendors differ, and investigate options based on size and market focus.

Market Definition

Security researchers have been warning development pros about SQL injection, cross-site scripting (XSS), and other code security weaknesses in their proprietary code since the late '90s, but developers are still writing insecure code. Sixty-nine percent of applications scanned in the last 12 months have at least one OWASP Top 10 flaw, and over 56% have at least one CWE Top 25 flaw, according to an [industry report](#). Forrester defines SAST as:

Tools that test and evaluate an application's proprietary code by examining the code or binary without executing the application. These products analyze the application or source code directly, including APIs and infrastructure configuration files, detecting where in the code security weaknesses exist.

SAST is a fundamental tool in application security to [secure what you sell](#), especially for organizations undergoing a development, security, and operations (DevSecOps) transformation. Organizations that automate and integrate SAST scanning early in the development lifecycle create a fast feedback loop for developers on their code when it is the most efficient to fix. This reduces unplanned work and allows developers to focus on business features and functionality.

Business Value

In [Forrester's 2022 data](#), web application exploits (e.g., SQL injection and XSS) were cited by 16% of global security decisions-makers as a method that was used to carry out an external attack at their company. Couple this with the 117% year-over-year increase in malicious API traffic reported [by Salt Security](#) and the unintentional open [S3 buckets that researchers](#) (and hopefully not attackers) find, and you'll see that organizations must continue to look for security flaws in their applications, APIs, and infrastructure as code (IaC) files. Security and development pros implement SAST to:

- **Reduce the time to fix application security weaknesses.** Organizations initially implement SAST to identify and remediate security flaws. But to reduce the time to fix issues, they must run SAST scans frequently and throughout the software development lifecycle (SDLC). Running scans on a defined schedule ensures all applications are tested but also overloads developers with flaws to wade through. This is not only inefficient when developers who have created the flaws have moved on, but it hurts morale. Development leaders are trying to balance the demand from security to fix security issues with the demand from product management to get new features out the door.

- **Improve application delivery speed and predictability.** DevOps methodology and tooling allow code to deploy faster than traditional waterfall lifecycle and operations playbook deployments. Twenty-six percent of global digital and IT professionals surveyed in [Forrester's Modern Technology Operations Survey, 2022](#), reported that their teams release frequently — monthly, weekly, daily, and even multiple times a day. To reduce the risk of security fire drills late in the release cycle, firms must implement SAST in the development phase so developers can find and fix security flaws while coding. Teams that run SAST in the IDE, on commit or pull requests, will better align to developers' speed requirements.
- **Prevent new weaknesses with fast feedback loops and secure coding education.** Developers are [not taught secure development in school](#); organizations must provide developers the tools and education. Giving developers feedback on their code while it is still fresh in their mind reduces remediation overhead and reinforces secure coding practices. This mimics how we learn in academia — there is a lecture from a professor and a hands-on lab that applies that learning. SAST tools that provide developers with real-time feedback and link to secure coding training reduce the potential for new application security tech debt backlog.

Market Maturity

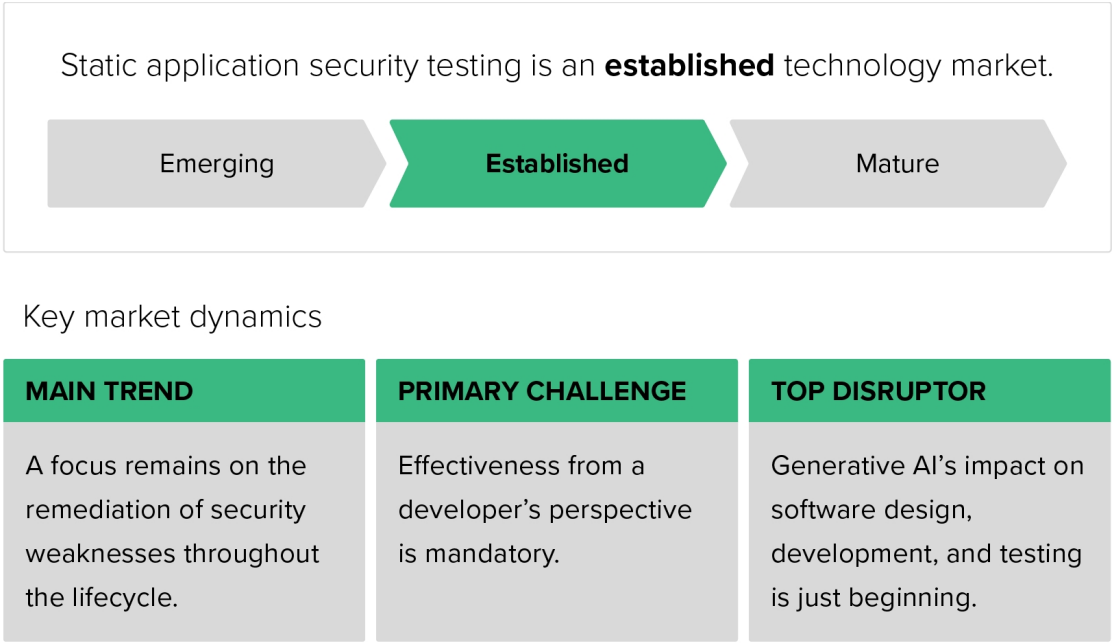
The SAST market has evolved as application development has advanced from a phased waterfall approach to an agile-plus-DevOps model with iterative coding and frequent deployment. To help developers release quality code faster, organizations are continuously introducing new architectures and technology stacks, developers are owning more of the application's infrastructure, and applications are increasingly a collection of distributed microservices deployed to cloud environments. This new reality pushes vendors of SAST (and other prerelease application security) tools to reinvent their implementation and rethink how these tools analyze applications (see Figure 1). SAST has evolved into an established market that:

- **Goes beyond assessing only code to a more holistic view of the app.** SAST tools are looking at more than just the application code to understand the IaC file. They're also looking at APIs, including ones not bundled with the application. Cloud, IaC, and containers are integral parts to modern development, and SAST results can now be enhanced by surfacing exploitability in runtime. In the past few years, software composition analysis (SCA) vendors have been using SAST to identify when a vulnerable method is called by the first-party code, making results

actionable. Cutting-edge SAST vendors flag coding patterns that consume more energy than others.

- **Takes a developer-centric approach.** SAST was once a tool run by security professionals in the late stages of development, and results were often sent in PDF form. Early attempts to retrofit SAST into build pipelines saw low developer adoption because of high volumes of false positives and long scan times. SAST vendors pivoted to a developer-centric approach and instead built tools that could be embedded in DevOps workflows directly and with less scan noise. SAST must continue to evolve to scan at the pace of code change and meet developers in their tools and deployment methods of choice.
- **Renewed interest from government on secure coding practices.** The [National Cybersecurity Strategy](#) seeks to shift liability for insecure software products and services to software makers, with a safe harbor protection for companies that securely develop and maintain them. The [executive order from May 2021](#) recommends SAST as part of secure software development processes. [CISA's April 13, 2023 security-by-design and -default guidance](#) reminds development teams to use SAST tools to “analyze product source code and application behavior to detect error-prone practices.”

Figure 1
Static Application Security Testing Market Maturity And Key Dynamics



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Market Dynamics

SAST has been around for years. Which begs the question, why is insecure code still being produced? One reason is that SAST tools continue to grapple with changes DevOps introduced. SAST tools were originally developed with security professionals in mind, providing out-of-the-box policies, reporting and analytics features, and reams of security defects to manage. Developers have never had time to wade through a backlog of issues to determine which were actionable or wait hours for a scan to complete so the continuous integration (CI) pipeline could move to the next stage. SAST quality gates in the CI/ continuous delivery (CD) pipeline essentially say to go back and fix the code, but do it on unaccounted-for time. The flip side is also true. Applications have a longer shelf life — longer than anyone in the business expects. The developer tasked with fixing the security issues is unlikely to have written the original code. DevSecOps touts collaboration, shared empathy, and collective responsibility. It is under this lens that SAST tools are evaluated, including what criteria is most important and what features make a tool successful in the market. Security and development pros will face a plethora of vendor options and should pay attention to

the following market dynamics.

- **Main trend.** A focus remains on the remediation of security weakness throughout the lifecycle. Code is constantly being modified, merged with other code, and assembled into larger applications. When SAST is run in the IDE or on a pull request, developers receive feedback in the context of the task at hand. Coupled with just-in-time, interactive training, this accelerates remediation and, more importantly, reinforces secure coding practices. Tools must also provide weakness information in a developer's language, highlight the vulnerable code, uplevel the quickest path to remediation, provide coding examples, and automate the remediation task.
- **Primary challenge.** Effectiveness from a developer's perspective is mandatory. Integrating scanning into the developer workflows leads to the highest adoption. What SAST surfaces to the developer must differ based on the stage in the lifecycle, the context of the application, and where the code will ultimately be executed. Tools will provide the best results when they can focus development work by only showing weakness introduced by their code change, use ML/AI to reduce false positives, speed up detection, provide code fixes, and correlate findings from multiple scan techniques to prioritize issues.
- **Top disruptor.** Generative AI's impact on software design, development, and testing is just beginning. Hobbyists and professionals can now use [ChatGPT to develop and test code](#). [Stanford researchers](#) showed that people using Github's copilot were more likely to write insecure code while conversely being confident in its security. These early pilots show that generative AI will affect proprietary code in unexpected ways that SAST tools will have to embrace. Vendors that have strong security research and AI/ML teams, a culture of continuous improvement, and a reputation for partnering with their customers will adapt best.

Notable Vendors

Security and development pros can start investigating specific vendors based on their market, with large vendors having over \$100 million, medium vendors having over \$30 million to \$100 million, and small vendors having \$10 million to \$30 million in product revenue (see Figure 2). They should also take into consideration geographic focus, industry focus, and type of offering (domain-specific solution/application or general-purpose platform).

Figure 2
The Static Application Security Testing Landscape, Q2 2023

Vendor	Geographic focus	Industry focus	Type of offering
LARGE >\$100M			
Checkmarx	NA; EMEA	Financial services Government High-tech products	General-purpose platform
OpenText	NA; EMEA; APAC	Financial services Government High-tech products	General-purpose platform
Synopsys ¹	NA; APAC	Financial services Government High-tech products	Domain-specific solution/application
Veracode	NA	Financial services High-tech products Professional services	General-purpose platform
MEDIUM >\$30M-\$100M			
Contrast Security ¹	NA	Financial services Healthcare Insurance	Domain-specific solution/application
Dersecur	EMEA; APAC	Financial services High-tech products Retail	Domain-specific solution/application
GitHub ¹	NA; EMEA	Financial services High-tech products Telecommunications	General-purpose platform
GitLab ¹	NA; EMEA	Financial services Government High-tech products	General-purpose platform
HCLSoftware ¹	NA; EMEA; APAC	Financial services Healthcare Insurance	Domain-specific solution/application

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Vendor	Geographic focus	Industry focus	Type of offering
MEDIUM >\$30M-\$100M			
Perforce Software ¹	NA; EMEA; APAC	High-tech products Industrial products Transportation	General-purpose platform
SonarSource ¹	NA; EMEA	Financial services Retail Healthcare	General-purpose platform
Snyk	NA; EMEA	Financial services High-tech products Retail	General-purpose platform
SMALL \$10M-\$30M			
Anpro-Xmirror Security	APAC	Financial services High-tech products Telecommunications	Domain-specific solution/application
Check Point ¹	NA; EMEA	Financial services Healthcare High-tech products	Domain-specific solution/application
Cycode	NA; EMEA	Financial services High-tech products Transportation	Domain-specific solution/application
GrammaTech ¹	NA; EMEA; APAC	Government High-tech products Transportation	General-purpose platform
Mend.io ¹	NA; EMEA	Financial services High-tech products Professional services	General-purpose platform
Offensive 360	EMEA	Financial services Government Professional services	Domain-specific solution/application

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Vendor	Geographic focus	Industry focus	Type of offering
SMALL \$10M-\$30M			
Parasoft ¹	NA; EMEA; APAC	Financial services High-tech products Transportation	Domain-specific solution/application
QI-ANXIN	APAC	Financial services Government Insurance	Domain-specific solution/application
Semgrep ¹	NA	Entertainment and leisure Financial services High-tech products	General-purpose platform
Sonatype	NA; EMEA	Financial services Government High-tech products	Domain-specific solution/application

Note: Geographic focus indicates regions where the vendor's product revenue in this category is greater than or equal to 15% of its total product revenue.

1. The vendor did not provide complete information for this table; this table includes Forrester's estimates.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Not Licensed For Distribution.

© 2023 Forrester Research, Inc. All trademarks are property of their respective owners.

For more information, see the [Citation Policy](#), contact citations@forrester.com, or call +1 866-367-7378.

Top Use Cases

We have identified the following core use cases for this market: identification of security weaknesses, DevSecOps, and remediation. These are the use cases most frequently sought after by buyers and addressed by SAST solutions. We have identified the following use cases as extended: policy and rules management, reporting and analytics, prioritization, quality, developer security education, governance, and application security posture. These are the use cases that some buyers look to address in addition to the core use cases; they’re less commonly addressed by SAST solutions (see Figures 3 and 4).



Figure 3
Static Application Security Testing: Core Use Cases

Use case	Objective	Top differentiators
Identification of security weaknesses	Identify security weaknesses in proprietary code	• Modern development support • SDLC integration • Rules customization
DevSecOps	Embed security into the development workflow to identify security weaknesses early and prevent new ones	• Automated remediation • Prioritization • IDE plug-ins, PR scanning • Integrated security developer education
Remediation	Help developers quickly remediate weaknesses	• Automated remediation • Prioritization • Integrated security developer education

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 4
Static Application Security Testing: Extended Use Cases

Use case	Objective	Top differentiators
Policy and rules management	Ensure applications meet the organization's risk tolerance for security	• Out-of-the-box policies • Custom policies • Rules customization
Reporting and analytics	Report on metrics, trends, and status specific to personas; get reports for compliance, internal, and regulatory requirements	• Audit, risk, and compliance reports • Remediation guidance and reporting • Integration with other app sec tools • Quality and/or sustainability metrics
Prioritization	Prioritize remediation and focus development resources	• Prioritization • Remediation guidance and reporting • Integration with other app sec tools • Custom policies
Quality	Analyze code for maintainability, relatability, and compliance	• Quality and/or sustainability metrics • Rules customization • SDLC integration • Integrated security developer education
Developer security education	Educate on secure coding techniques, common weaknesses, and security tooling	• Remediation guidance and reporting • Integrated security developer education • SDLC integration
Governance	Provide evidence that application security validation was conducted prior to production deployment	• Out-of-the-box policies • Audit, risk, and compliance reports • Quality and/or sustainability metrics
Application security posture	Understand the overall security posture of an application by incorporating analysis from other security tools and production	• Prioritization • Integration with other app sec tools • Audit, risk, and compliance reports

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Functionality By Use Case

Even though the SAST market has been around for a number of years, vendors are differentiating by the large number of extended use cases. Select the use cases that are most relevant to your business requirements and then use the following tables as a guide to choose the functionalities that matter most for your technology evaluation and vendor selection criteria (see Figures 5 and 6).

Figure 5
Static Application Security Testing: Functionality By Core Use Case

Functionality	Identification of security weaknesses	DevSecOps	Remediation
Flaw and vulnerability detection	●	●	●
Prioritization	○	●	●
Out-of-the-box policies	●	○	○
Custom policies	●	○	○
Audit, risk, and compliance reports	○	●	○
Remediation guidance and reporting	●	●	●
Automated remediation	●	●	●
Modern development support	●	●	●
Integrated security developer education	○	●	○
SDLC quality gates	●	●	●
IDE plug-ins, PR scanning	●	●	●
SDLC integration	●	●	○
Rules customization	●	●	●
Integration with other app sec tools	○	○	○
Quality and/or sustainability metrics	●	●	●

● Primary functionality required for a given use case

○ Secondary functionality required for a given use case

● Little to no functionality required for a given use case

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 6
Static Application Security Testing: Functionality By Extended Use Case



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Extended Use Cases By Vendor

Organizations with a developer focus should consider prioritization and secure coding education, while organizations that need insight into overall business risk should look at application security posture extended use cases. We asked each vendor included in this report to select its top use cases for which customers select that vendor’s product. From this, we determined the extended use cases that highlight differentiation among vendors. The following table shows how each vendor’s responses map to those. This table represents the vendor-reported use cases for which clients select them, not

Not Licensed For Distribution.
© 2023 Forrester Research, Inc. All trademarks are property of their respective owners.
For more information, see the [Citation Policy](#), contact citations@forrester.com, or call +1 866-367-7378.

available functionalities (see Figure 7).



Figure 7
Static Application Security Testing: Extended Use Case By Vendor

Vendor	Policy and rules management	Reporting and analytics	Prioritization	Quality	Developer security education	Governance	Application security posture
Anpro-Xmirror Security		●					●
Check Point					●		●
Contrast Security		●	●				●
Cycode	●		●				●
Dersecur		●	●	●			●
GitHub	●	●	●		●		
GitLab	●	●			●	●	●
GrammaTech		●		●			
HCLSoftware	●		●			●	●
Mend.io	●	●	●				●
Offensive 360		●		●	●		●
OpenText	●		●		●		●
Perforce Software	●	●		●	●		●
QI-ANXIN		●	●				

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Vendor	Policy and rules management	Reporting and analytics	Prioritization	Quality	Developer security education	Governance	Application security posture
Semgrep	●		●				●
Snyk		●	●		●		●
SonarSource	●			●	●		
Sonatype	●	●	●		●		
Synopsys	●		●	●			

Note: The following vendors selected most or all use cases in our questionnaire: Checkmarx and Veracode.
Note: The following vendor declined to provide use case information in our questionnaire: Parasoft.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Supplemental Material

Methodology

To complete our review, Forrester requested information from vendors. If vendors didn't share this information with us, we made estimates based on available secondary information. We've marked all estimates with a note. Forrester fact-checked this report with vendors before publishing.

Companies We Researched For This Report

Forrester researched the following companies for this report.

- Anpro-Xmirror Security
- Checkmarx
- Check Point
- Contrast Security
- Cycode
- DerSecur
- GitHub
- GitLab
- GammaTech

HCLSoftware

Mend.io

Offensive 360

OpenText

Parasoft

Perforce

QI-ANXIN

Semgrep

Snyk

SonarSource

Sonatype

Synopsys

Veracode



We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

[Learn more.](#)

Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

[Learn more.](#)

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

[Learn more.](#)

FOLLOW FORRESTER



Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com