Red River | Checkmarx

TD SYNNEX Public Sector | DLT

APPLICATION SECURITY TESTING TOOLS: A BUYERS GUIDE

Application development is a complex process requiring planning, design, usability and testing to ultimately deliver a functional solution. While applications are designed to increase organizational efficiency to support critical tasks, they are marked by two key challenges: security and integration. Simply put, application risk is business risk. Organizations have to keep security front and center through the entire development workflow, as vulnerabilities in the development process can create mission-critical risk to users and the organization as a whole. Integrating application development tools into the existing technology landscape, and meeting time and regulatory requirements compound the process, which has made development an area of focus for organizations that struggle to balance the time, cost and effectiveness of this process.

The market for application security testing is forecasted to grow 11.8% over the next eight to ten years due to the rise in cyber attacks.

The market for application security testing is forecasted to grow 11.8% over the next eight to ten years due to the rise in cyber attacks. Organizations are essentially being forced to find their security vulnerabilities before criminals do.

Speed in application development is a competitive advantage, but only if that development creates an outcome free of security risks and other issues.

Static Application Security Testing (SAST) tools have been instrumental in early software development stages to implement security testing before deployment so developers can refine new features and remediate potential issues without sinking too many resources. However, most major tools are not easy to use and developers aren't traditionally trained in security, leaving them to "learn as they go." This results in cumbersome administrative processes and avoidance of key security tasks necessary to success.

Gaining Advantage for Development Teams Starts with the Right SAST Tool

There are numerous SAST tools providing a range of features on the market today. Most organizations have some form of AST process or tool in place. As decision makers consider their modernization goals, many times the rising costs of renewals for existing tools creates a larger conversation about what's practical and possible in the world of SAST. In some cases, renewal is the best option; in others, a rip and replace approach (even one that is phased out over time) can prove to be more cost-effective and provide additional features and functionality not previously available. As leaders evaluate the true cost of modernization, it's prudent to look back at historical tech debt with the legacy tool and how much the solution has aided in or detracted from an efficient development process. Here are some key things to look for:

1. Ease of Integration

Overall, SAST tools should aim to limit impact on the developer and improve progress toward development deadlines. When a new tool is introduced, it often requires teams to change their approach. However, expecting a tool to be successful while also asking developers to change behaviors in order to make it successful is typically not effective. It is essential to provide developers a pathway to improve productivity with tools that integrate directly into the existing workflow to help secure code quickly without having to reset. A good SAST tool should integrate all the elements listed on the following page.

- Source Code Management (SCM) Solutions (eg: GitLab, GitHub, Bitbucket)
- Integrated Development Environment (IDE) Solutions (eg: Visual Studio, IntelliJ, Eclipse)
- Continuous Integration/Continuous Delivery (CI/CD) Solutions (eg: Team City, Bamboo, CircleCI, Jenkins)
- Feedback Solutions (eg: Rally, Jira, Azure DevOps)

Tools with this kind of integration versatility truly "meet developers where they are" so they can focus on the technical goal, not the administration.

2. Ease of Automation

Tools that automate actions create more efficiency and improve adoption. Tools that can automatically resolve issues reduce the need for manual intervention and quickly detect/prioritize vulnerabilities eliminate administrative work for the developer and support team. SAST tools check code against security best practices and coding standards to identify deviations so developers adhere to secure coding practices. Standards can be customized in the tools to set a benchmark for deployment.

> **Tools that can automatically resolve issues reduce the need for manual intervention, and detect and prioritize them more quickly.**

Tools that can automatically scan large volumes of code save time by identifying issues earlier in the process – providing insights for improvement along the way. Automation also reduces human error and allows organizations to scale more easily when facing the complexity of developing and launching larger applications. Some tools allow users to schedule vulnerability scanning when compute resources aren't being used at night and enable "triggers" that raise key concerns throughout the process, so the development team doesn't have to think about them at each step. This creates an efficiency advantage across the organization. Tools that prioritize automation across ticket management and provide practical remediation guidance in response to auto scanning can dramatically lighten the administrative load across development and security teams.

3. COTS Product Testing

Tools that leverage this automation approach can reduce the amount of time between the security team identifying issues to sharing those vulnerabilities back to the developers. Another application for this capability in federal environments is with testing emerging technologies. When agencies are exploring different commercial solutions and applications that they might be able to incorporate in their solution sets, some SAST tools can scan, ingest and then approve these tools from a security standpoint to be integrated into the network. Provided that the COTS owners can provide the source code, SAST tools can be effective in identifying if there is additional development needed to meet requirements. Essentially, these tools can shorten the process of establishing compliance with zero trust models and other security protocols to fast-track deployment.

4. Reduced Time to Remediation

With some SAST tools, a developer will open a report from a scan and see a long list of vulnerabilities they don't have the time or experience to troubleshoot. As this will create technical debt specific to security when deployed, the project will be forced to shut down non-compliant features. Building in security scans up front reduces security debt and leveraging tools that prioritize and suggest remediation enables teams to fix issues based on severity, whether it's exploitable and how critical it is to the organization. Running automated security scans early and often in the SDLC saves time, speeds up DevOps processes and helps organizations achieve authorization to operate (ATO).

Simplified vulnerability management for some tools can even extend across all application security solutions.

5. User Experience & Reporting

The experience for developers is paramount. A tool is only helpful if it streamlines and simplifies. Providing easy-to-understand reports with remediation guidance and instruction that is comprehensive and easy to follow changes the speed and accuracy of development. Dashboards that favor customizable report creation, scheduled report generation, and analysis of data and scan results make the process easier to digest and actionable for teams that are focused on meeting deadlines versus security management. Reporting can either add time to the process or reduce it, making it a critical decision factor for choosing a SAST solution.

SAST should be designed to build trust and provide support with a deep security layer to step through and automate remediation regardless of security expertise – making it easy for the developer to fix any issues and learn from these fixes to improve development in the future. Simplified vulnerability management for some tools can even extend across all application security solutions, allowing teams to triage and share risks with development in a single workflow to reduce complications.

True Agile Development Means Building in Security from Step One

As organizations drive to stay true to agile development philosophies, zero trust initiatives and growing cybersecurity standards, building in security and remediation efforts from the beginning has become the gold standard. Red River and Checkmarx support customers in meeting the demands of the application and workload pillar of the Zero Trust imperative, with the Checkmarx SAST solution fulfilling 16 of these activities.

Checkmarx provides public sector agencies with a comprehensive AST Platform and on-premises AST solutions that allows them to protect their applications early, quickly and cost-efficiently. With it, federal, state and local governments, and education institutions can effectively meet compliance regulations and embed security throughout the SDLC to prevent security breaches and enhance Zero Trust initatives. Checkmarx helps to optimize DevSecOps programs with automated security scans, intelligent remediation, risk severity scoring, simplified reporting and integrated developer training. Checkmarx SAST is an on-premise solution that prioritizes developer adoption and integration within existing workflows to improve outcomes, reducing the number of vulnerabilities for remediation by 50%. With 100 billion lines of code scanned monthly and support for more than 75 languages and technologies, Checkmarx seamlessly integrates into any development environment.

With a full suite of solutions based on the size and scale of the organization, Checkmarx One consolidates multiple market-leading AppSec solutions into a single, unified platform with the ability to manage hundreds of apps and thousands of individual projects. It is built on the cloud and for the cloud. Checkmarx' updated analytics and reporting provides the data necessary to influence stakeholders, build trust, and make organizations more secure.

For more information about leveraging the right SAST tool for your organization, contact **info@redriver.com**

TD SYNNEX Public Sector | DLT

Checkmarx

ABOUT CHECKMARX FOR PUBLIC SECTOR

Checkmarx is the leader in application security and ensures that enterprises worldwide can secure their application development from code to cloud. Our consolidated platform and services address the needs of enterprises by improving security and reducing TCO, while simultaneously building trust between AppSec, developers, and CISOs. At Checkmarx, we believe it"s not just about finding risk, but remediating it across the entire application footprint and software supply chain with one seamless process for all relevant stakeholders.

We are honored to serve more than 1,800 customers, which includes 60 percent of all Fortune 100 companies including Siemens, Airbus, SalesForce, Stellantis, Adidas, Wal-Mart and Sanofi. For more information, visit **checkmarx.com**.

Red River

ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing more than 25 years of experience and mission-critical expertise in managed services, cybersecurity, modern infrastructure, collaboration and cloud solutions.

Learn more at **redriver.com**.