First Choice Tools: A Practical Comparison

Category	Tool Name	License / Pricing	Pros	Cons	Supported Languages	Comments
SAST	SonarQube	• Open source (LGPL v3) • Free Community Edition for basic security/quality checks • Paid plans unlock advanced security rules and additional languages	Comprehensive code quality and security checks. Built-in rules and quality gates. Supports multiple languages. Central dashboard for code health.	Requires self-hosting or Docker. Some advanced security features are available only for paid editions.	Over 25 languages (Java, C#, JavaScript, TypeScript, Python, etc.).	Good if you want combined code quality and security. Docs at https://docs.sonarqube.org.
	Semgrep	• Open source (GPL-2.0+) - not recommended as a SAST tool • Free Semgrep Cloud tier: up to 10 contributors for private repos, unlimited for public • Paid plan for larger organizations ($40 per contributor/month)	Lightweight and fast. Highly customizable rule engine. Extensive community rule library. Easy CI integration (GitHub, GitLab, etc.).	May produce false positives if rules are broad. Writing custom rules requires learning Semgrep's syntax. Free cloud tier limited to 10 unique contributors for private code.	Wide range: Python, Java, JavaScript, TypeScript, Go, C/C++, Ruby, etc.	Ideal for quick, targeted scans across multiple languages. Semgrep open source has several significant limitations and doesn't qualify as a SAST tool. Docs at https://semgrep.dev/docs.
SCA	Dependabot (GitHub)	• Free for GitHub repositories	Native GitHub integration. Automated PRs keep dependencies updated. Minimal configuration.	Limited to GitHub only. Customization can be tricky.	Major package managers: Node.js, Python, Ruby, Java, .NET, etc.	Great for seamless dependency updates in GitHub. Docs at https://docs.github.com/code-security/dependabot.
	Snyk	• Free plan, limited to 200 tests per month • Team plan up to 10 developers ($25 per dev/month) • Enterprise plan - custom pricing	Extensive vulnerability database. Simple CI/CD integration. Covers multiple ecosystems (Docker, JS, Python, etc.).	Free tier has monthly scan limits for private repos. Advanced features (like license compliance) require a paid plan. Pricing can increase with extensive usage.	Many (Java, .NET, Python, JavaScript, Ruby, Go, PHP, etc.).	Ideal for user-friendly SaaS with a good free tier. Docs at https://docs.snyk.io.
DAST	OWASP Zed Attack Proxy (ZAP)	• Open source (Apache 2.0). Completely free with full functionality.	Community-driven (OWASP). Automated and manual pentesting modes. Extension marketplace and good docs. Ideal for OWASP Top 10 testing.	The interface can be complex for newcomers. Requires Docker/CLI setup in CI. Automated scans may miss logic flaws (manual testing recommended).	Scans running web apps via HTTP/HTTPS.	Great free DAST solution with a strong community. Docs at https://www.zaproxy.org/docs.
	Burp Suite Enterprise Edition	• Commercial (custom pricing)	Fully automated scanning with scheduled tests. Integration with CI/CD pipelines. Scalable for large applications.	High cost compared to open-source alternatives.	Language-agnostic (scans web applications via HTTP/HTTPS).	Great for organizations needing continuous web application security scanning at scale. Docs at https://portswigger.net/burp/documentation
Container / IaC Scanning	Trivy	• Open source (Apache 2.0). Free with no usage limits. Maintained by Aqua Security	Scans containers and IaC (Terraform, Kubernetes, etc.). Fast, easy to run locally or in CI. Strong community updates.	Advanced use cases may need manual config. Requires Docker or a container environment for container scanning.	Focuses on container images, Terraform, Kubernetes manifests, etc.	Excellent all-in-one vulnerability scanner for cloud-native apps. Docs at https://trivy.dev/latest/docs/
	Checkov	• Open source (Apache 2.0). Free with no usage limits.	Focused IaC security with an extensive policy library. Integrates well with GitHub/GitLab. Covers Terraform, CloudFormation, Kubernetes, etc.	May require custom policies for unique setups.	Terraform, CloudFormation, Kubernetes, Azure Resource Manager, etc.	Great for detecting misconfigurations in IaC. Docs at https://www.checkov.io/1.Welcome/Quick%20Start.html