How Technology Can Help us Shift Security to the Left

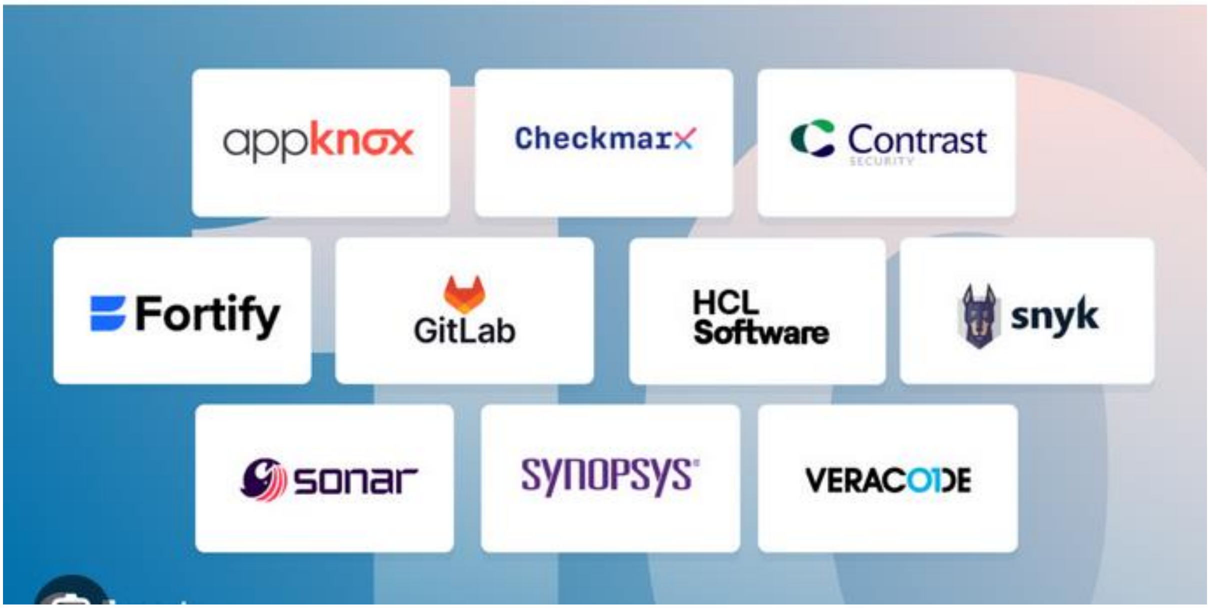
As mentioned, part of a good shift left strategy, especially for enterprises, is leveraging the available tools for testing. Each tool serves a different purpose and tests the product differently.

Technology plays a crucial role in shifting security to the left by providing tools and automation that enable developers to identify and address security issues earlier in the software development life cycle (SDLC). Some ways technology can help with shift left security include:

Static Application System Testing (SAST)

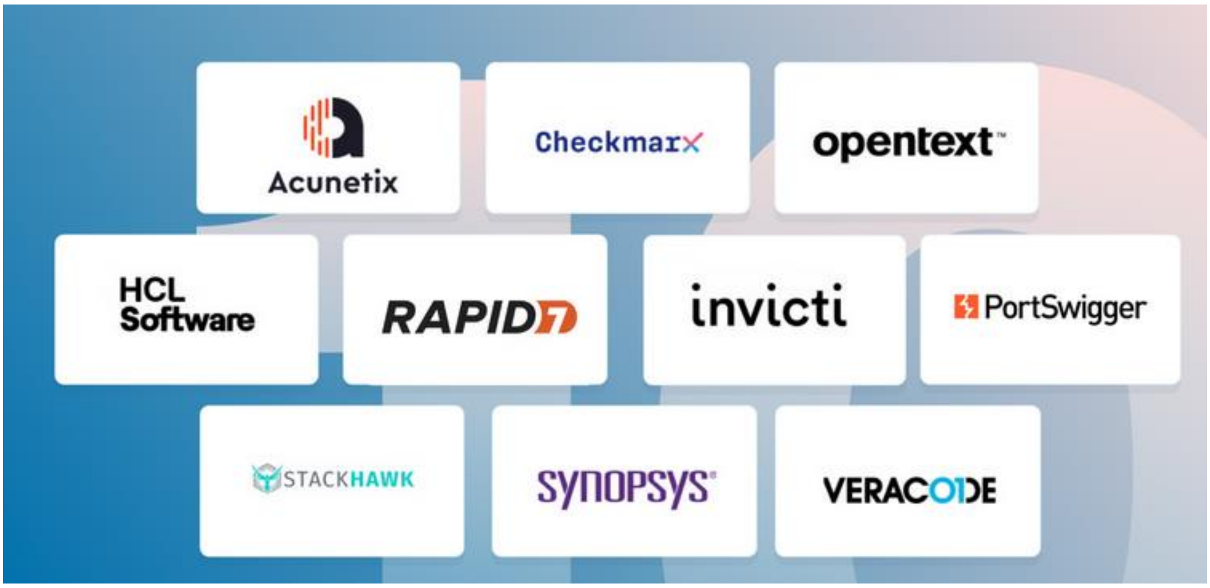
SAST is used to scan the source code itself for vulnerabilities. This is referred to as white-box testing, and the results include recommendations for remediation of any discovered issues. This kind of testing is the earliest that can be initiated in shift left security.

The Top 10 Static Application Security Testing (SAST) Tools include:



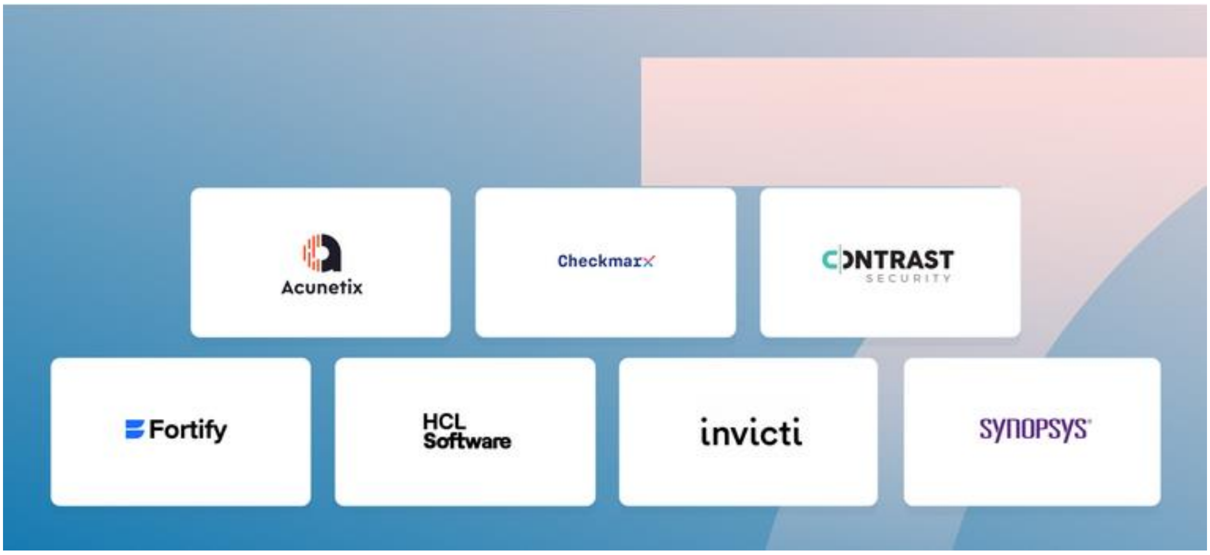
Dynamic Application Security Testing (DAST)

DAST is a kind of black-box testing, where the application in development is exposed to a variety of common attacks. The results may indicate security vulnerabilities as well as runtime configuration issues.



Interactive Application Security Testing (IAST)

IAST is a hybrid marriage of SAST and DAST. It analyzes the application under development and monitors its behavior when exposed to a series of manual and automated tests simulating attacks within a controlled sandbox.



Runtime Application Self-Protection (RASP)

RASP runs in integration with the application during runtime to prevent attacks. It blocks execution based on either user behavior or traffic.

CONTRAST SECURITY
DATADOG
dynatrace
Fortify
imperva
Signal Sciences

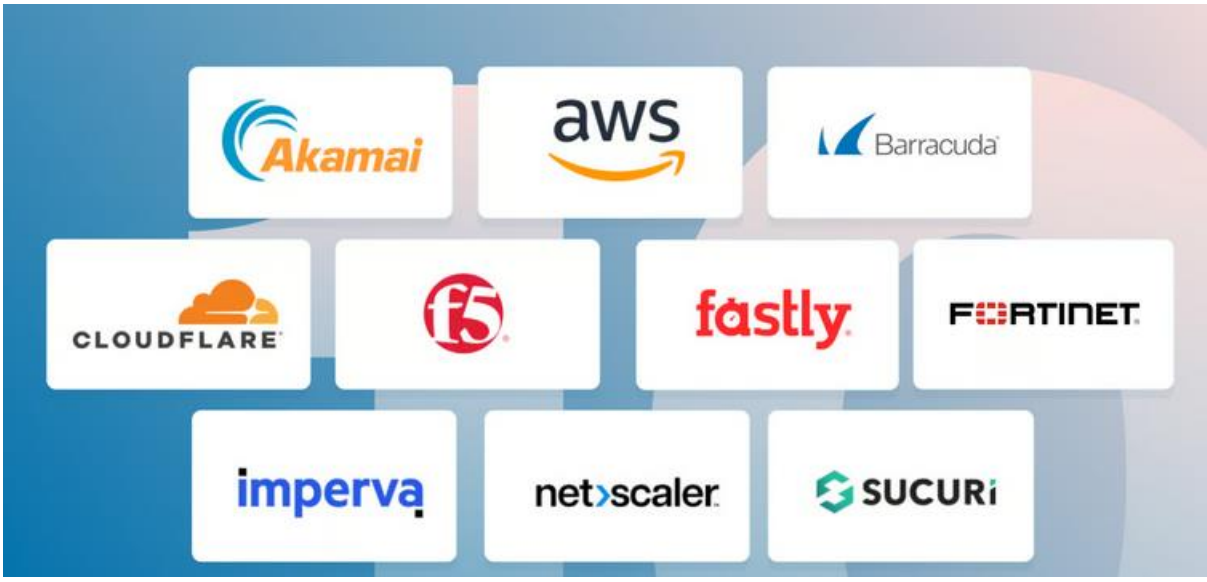
Software Composition Analysis (SCA)

SCA is an automated tool for cataloging and analyzing open-source components used in software development. It scans for licensing issues, build versions, dependencies, and vulnerabilities, and it can be used to manage those components throughout the SDLC.

CAST Software Intelligence for Digital Leaders
Checkmarx
FOSSA
GitLab
JFrog
mend.io
snyk
sonatype
SYNOPSYS
VERACODE

Web Application Firewalls (WAF)

WAFs monitor and protect web applications against a variety of threats, such as malware and zero-day exploits. They block any malicious HTTP/HTTPS traffic that attempts to compromise the web application security.



Conclusion:

By implementing these technologies, organizations can improve their security posture and reduce the risk of vulnerabilities in their applications, thereby adhering to the principles of DevOps and DevSecOps cultures, which emphasize the integration of security throughout the development process.