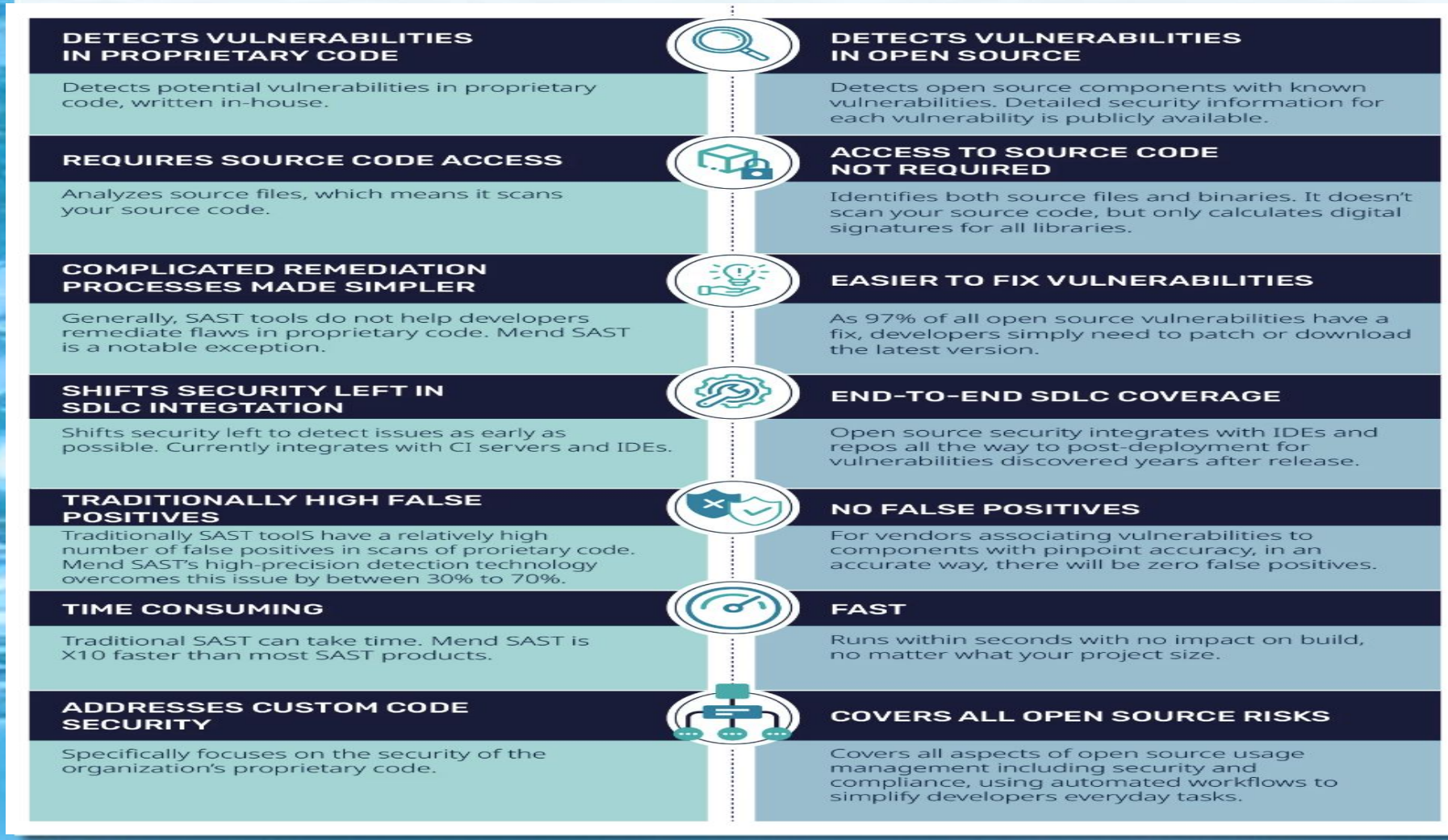
SCA SECURITY

Software Composition Analysis

SCA is an application security methodology that focuses on scanning applications for the open source dependencies being used, either directly or indirectly, and correlating this analysis with vulnerability data to track any known security vulnerabilities these dependencies might include.

SCA also helps map the legal risk introduced via open source usage by identifying the licenses included in open source packages.

SAST VS SCA


DETECTS VULNERABILITIES IN PROPRIETARY CODE
Detects potential vulnerabilities in proprietary code, written in-house.
DETECTS VULNERABILITIES IN OPEN SOURCE
Detects open source components with known vulnerabilities. Detailed security information for each vulnerability is publicly available.
REQUIRES SOURCE CODE ACCESS
Analyzes source files, which means it scans your source code.
ACCESS TO SOURCE CODE NOT REQUIRED
Identifies both source files and binaries. It doesn't scan your source code, but only calculates digital signatures for all libraries.
COMPLICATED REMEDIATION PROCESSES MADE SIMPLER
Generally, SAST tools do not help developers remediate flaws in proprietary code. Mend SAST is a notable exception.
EASIER TO FIX VULNERABILITIES
As 97% of all open source vulnerabilities have a fix, developers simply need to patch or download the latest version.
SHIFTS SECURITY LEFT IN SDLC INTEGTATION
Shifts security left to detect issues as early as possible. Currently integrates with CI servers and IDEs.
END-TO-END SDLC COVERAGE
Open source security integrates with IDEs and repos all the way to post-deployment for vulnerabilities discovered years after release.
TRADITIONALLY HIGH FALSE POSITIVES
Traditionally SAST toolS have a relatively high number of false positives in scans of prorietary code. Mend SAST's high-precision detection technology overcomes this issue by between 30% to 70%.
NO FALSE POSITIVES
For vendors associating vulnerabilities to components with pinpoint accuracy, in an accurate way, there will be zero false positives.
TIME CONSUMING
Traditional SAST can take time. Mend SAST is X10 faster than most SAST products.
FAST
Runs within seconds with no impact on build, no matter what your project size.
ADDRESSES CUSTOM CODE SECURITY
Specifically focuses on the security of the organization's proprietary code.
COVERS ALL OPEN SOURCE RISKS
Covers all aspects of open source usage management including security and compliance, using automated workflows to simplify developers everyday tasks.

SCA + SAST SECURITY

Solution :

An effective application security approach, therefore, should seek to include security testing tools capable of managing and mitigating both types of risk.

Tools eg.

Gitlab

Github

Snyk

Sonatye NexusIQ