Mend SAST

Security at the Speed of DevOps

The Challenge

As enterprise security managers increasingly focus on risk management over compliance, many turn to Static Application Security Testing (SAST) tools to identify security vulnerabilities in the custom code written by application developers. Unfortunately, most SAST tools end up sitting on the proverbial shelf collecting dust, because they are a poor fit for modern fast-paced development environments.

Traditional SAST tools are famous for being:

Cumbersome - They often require specialized expertise to configure and force developers to leave their development environment to trigger the scan, view results, and research the fix.

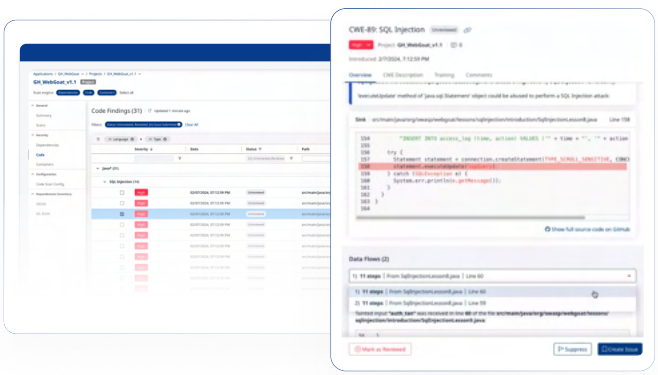
Slow to produce results - Traditional SAST tools typically take hours to run, and sometimes even more. This is a poor fit for DevOps teams whose release cycles — from code commit to application deployment— are only getting tighter.

Limited in scope - They do not support all the diverse programming languages that are used in modern application development.

The Solution

Mend SAST is a breakthrough product that empowers enterprise application developers to create new applications with speed and confidence—without compromising security. This powerful Static Application Security Testing (SAST) solution enables developers to find and fix security vulnerabilities within their proprietary code quickly and accurately.

With scan speeds that are 10 times faster than legacy SAST solutions, Mend SAST integrates effortlessly into your existing development workflows. This provides your team with immediate feedback, actionable remediation guidance, and contextual education—all within their preferred development environments.



Why Mend SAST?

Speed

Up to 10 times faster than traditional SAST solutions, Mend SAST can be triggered with every code commit, so you can identify risks before they take the lead.

Repo-centric approach

Stop sifting through mountains of SAST findings. Mend SAST shows developers new findings from their last commit—in their own repo and in near real time—with actionable remediation guidance.

Data flow consolidation

Using advanced data flow consolidation, Mend SAST eliminates redundant alerts, cutting down on excess noise.

Hybrid cloud solution

By scanning locally and performing analysis in the cloud, Mend SAST gives you peace of mind that source code is not leaving your premises, combined with fast deployment and low maintenance.

Holistic training

Mend SAST is integrated with Secure Code Warrior to give your developers the just-in-time correction and security training they need.

What you get from Mend SAST: Features & Capabilities

Security teams choose Mend SAST for its unique capabilities, including:

Easy integration - Mend SAST integrates easily with existing DevOps environments and CI/CD pipelines, so developers don't need to separately configure or trigger the scan.

Optimized workflow - Mend SAST includes a wide range of scanning configuration options to create a best fit for each project, plus a detailed dashboard that connects you to user-friendly reporting, analytics, issue ticketing, and more

Extensive language support - Mend SAST supports 27 different programming languages and various different programming frameworks.

Ensure Compliance - Built-in reports for security standards such as PCI and HIPAA allow you to easily meet compliance requirements.

Integrations

Jenkins

Github

Azure DevOps

Bamboo

Teamcity

Bitbucket

GitLab

Jira

Secure Code Warrior

About Mend.io

Trusted by the world's leading companies, including IBM, Google, and Capital One, Mend.io's enterprise suite of application security tools is designed to help you build and manage a mature, proactive AppSec program.

Mend understands the different AppSec requirements of developers and security teams. Unlike other AppSec solutions that force everyone to use a single tool, Mend helps them work in harmony by giving each team different, but complementary, tools—enabling them to stop chasing vulnerabilities and start proactively managing application risk.

Learn more at