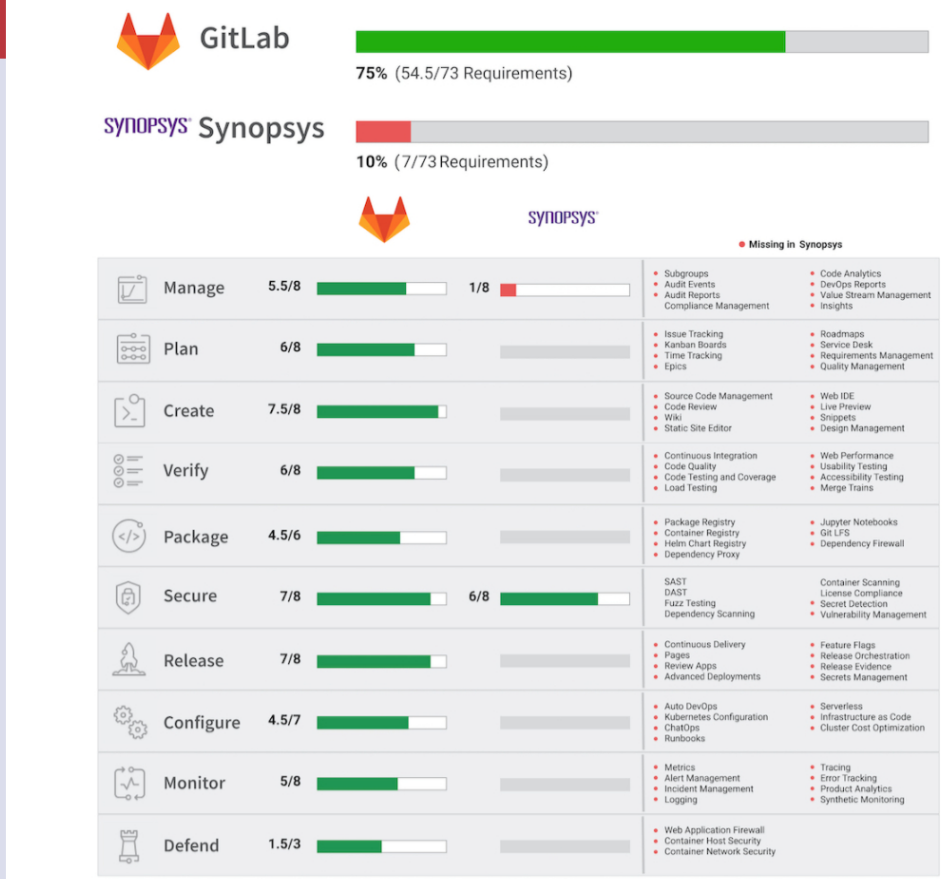
GitLab vs Synopsys

Decision Kit

Download Comparison



Summary

Synopsys owns a portfolio of several scanning tools, including Coverity (SAST), Black Duck (SCA), Seeker (IAST), Defensics (Fuzzing), and recently acquired Tinfoil (DAST).

BlackDuck does Software Composition Analysis (SCA) including dependency scanning, container scanning, and license management. BlackDuck maintains an Inventory of all open source code and its vulnerabilities and makes it available in the CI/CD pipeline via APIs. Unlike GitLab, it can detect more granular components beyond library use. BlackDuck can say if the part of the dependency used is exploitable. BlackDuck covers 81 languages.

Coverity for SAST includes spell-checker-like capability with an IDE plug-in that alerts the developer to vulnerable phrases as they code. It also has a dashboard that pulls in IAST from Seeker for a unified view. Coverity covers 20 programming languages. Our research indicates that Coverity costs around $12k USD per year for 5 users.

Seeker for IAST employs an agent to test the application for vulnerabilities. It is used during functional testing so that security tests are done in the normal course of other testing. Seekers has an API to integrate with Dev IDEs. Seeker works with Java/all JVM languages. Seeker is only available on premise.

Comparison to GitLab

GitLab Ultimate automatically includes a full suite of broad security scanning with every code commit. GitLab's scan results are provided to the developer inline in their Merge Requests with no integration required. GitLab security scanning includes not only SAST and DAST but also Container and Dependency scanning, License Compliance scanning, and Secrets detection. All of these are included in GitLab Ultimate and integrated directly into the developer's workflow. Finding vulnerabilities is only the beginning. Delivering those findings to the developer for immediate remediation is key to shifting left to reduce both cost and risk.

GitLab Strengths * Tool management is much simpler as it is all included in a single tool. * Vulnerabilities surfaced for the developer in their CI pipeline for immediate remediation. * Visibility of security risks throughout the SDLC. * Suggested Solutions * Easy onboarding

Synopsys Strengths * Recognition as a security testing leader by Gartner. * Managed services offering for customers who are looking to outsource their security scanning. * Polaris Software Integrity Platform provides a single console to manage all of Synopsys' testing products. * Integration with

IDEs and local developer environments beyond GitLab.

Feature Comparison

FEATURES	SYNOPSYS	GitLab
Static Application Security Testing CORE STARTER PREMIUM ULTIMATE FREE BRONZE SILVER GOLD GitLab allows easily running Static Application Security Testing (SAST) in CI/CD pipelines; checking for vulnerable source code or well known security bugs in the libraries that are included by the application. Results are then shown in the Merge Request and in the Pipeline view. This feature is available as part of Auto DevOps to provide security-by-default. Learn more about Static Application Security Testing	✓ supports 20 languages	✓ supports 18 languages
Secret Detection CORE STARTER PREMIUM ULTIMATE FREE BRONZE SILVER GOLD GitLab allows you to perform Secret Detection in CI/CD pipelines; checking for unintentionally committed secrets and credentials. Results are then shown in the Merge Request and in the Pipeline view. This feature is available as part of Auto DevOps to provide security-by-default. Learn more about Secret Detection	✗	✓
Dependency Scanning CORE STARTER PREMIUM ULTIMATE FREE BRONZE SILVER GOLD GitLab automatically detects well known security bugs in the libraries that are included by the application, protecting your application from vulnerabilities that affect dependencies that are used dynamically. Results are then shown in the Merge Request and in the Pipeline view. This feature is available as part of Auto DevOps to provide security-by-default. Learn more about Dependency Scanning	✓	✓
Container Scanning CORE STARTER PREMIUM ULTIMATE FREE BRONZE SILVER GOLD When building a Docker image for your application, GitLab can run a security scan to ensure it does not have any known vulnerability in the environment where your code is shipped. Results are then shown in the Merge Request and in the Pipeline view. This feature is available as part of Auto DevOps to provide security-by-default. Learn more about container scanning	✓	✓
Dynamic Application Security Testing CORE STARTER PREMIUM ULTIMATE FREE BRONZE SILVER GOLD Once your application is online, GitLab allows running Dynamic Application Security Testing (DAST) in CI/CD pipelines; your application will be scanned to ensure threats like XSS or broken authentication flaws are not affecting it. Results are then shown in the Merge Request and in the Pipeline view. This feature is available as part of Auto DevOps to provide security-by-default. Learn more about application security for containers	✓	✓
Interactive Application Security Testing CORE STARTER PREMIUM ULTIMATE FREE BRONZE SILVER GOLD IAST combines elements of static and dynamic application security testing methods to improve the overall quality of the results. IAST typically uses an agent to instrument the application to monitor library calls and more. GitLab does not yet offer this feature.	✓	✗
License Compliance CORE STARTER PREMIUM ULTIMATE FREE BRONZE SILVER GOLD Check that licenses of your dependencies are compatible with your application, and approve or deny them. Results are then shown in the Merge Request and in the Pipeline view. Learn more about License Compliance	✓	✓
On-demand Dynamic Application Security Testing CORE STARTER PREMIUM ULTIMATE FREE BRONZE SILVER GOLD "There's no reason to wait for the next CI pipeline run to find out if your site if vulnerable or to reproduce a previously found vulnerability. GitLab offers scanning your running application with On-demand Dynamic Application Security Testing (DAST), independent of code changes or merge	✓	✓

requests."

Learn more about On-demand DAST

Get Your Free Trial