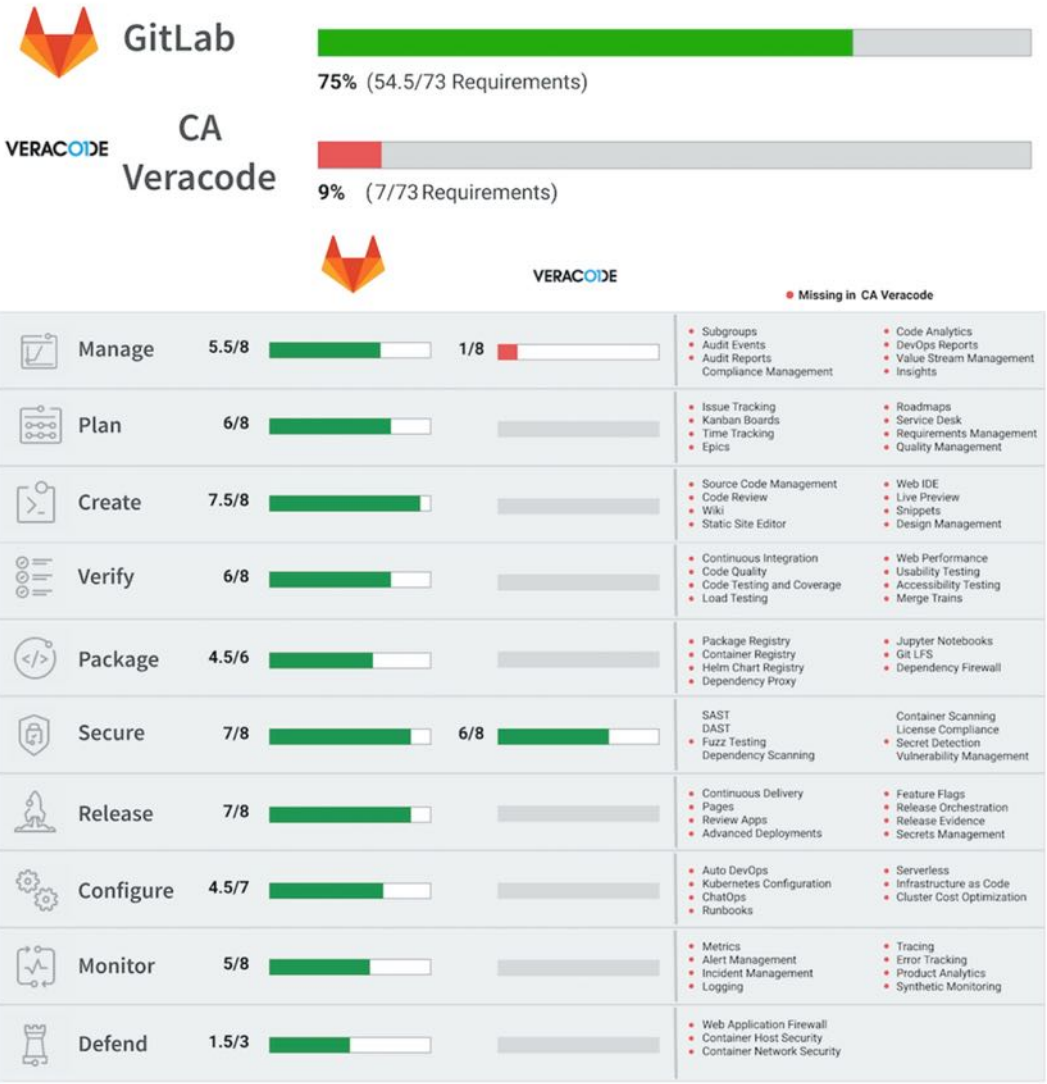
GitLab vs Veracode

Decision Kit



Summary

Both Veracode and GitLab Ultimate offer open source component scanning along with Static and Dynamic Application Security Testing. Veracode is a mature product with a hefty price tag. Veracode offers a separate SAST-lite product that integrates in the developer's IDE offering spell-check-like functionality to flag vulnerabilities as the developer types.

GitLab Ultimate automatically includes broad security scanning with every code commit including Static and Dynamic Application Security Testing, along with dependency scanning, container scanning, and license management.

Note: In November 2018, the private equity firm Thoma Bravo acquired Veracode from Broadcom. Veracode now functions as an independent company within the Thoma Bravo portfolio of companies. Between March 2017 and July 2018 Veracode was part of CA Technologies. For a brief period, from July 2018 to November 2018, Veracode was part of Broadcom following CA Technologies' acquisition by Broadcom

Comparison to GitLab

Veracode is a well established player in the Application Security Testing (AST) market. Although they offer a range of products, including SAST, DAST, IAST, and SCA, each of these products are sold and licensed separately. GitLab offers simplicity and a high level of integration by including all of these types of scanning capabilities within a single product. Additionally, GitLab has tightly integrated the scanning results with the rest of the SLDC, including the merge request review process.

Additionally, organizations that have concerns about using a cloud-hosted scanning solution, or that use GitLab's self managed offering, will find that GitLab is a clear winner as Veracode does not have an on-premise offering.

Security Scanning

Strengths and Weaknesses

	GitLab	Veracode
Strengths	• Tight out-of-the-box integration with the rest of the SDLC, including the merge request review process • GitLab's recent acquisitions of Peach Tech and Fuzzit provide Fuzzing capabilities that Veracode lacks • Supports on-premise deployments including disconnected, offline, or air-gapped environments	• Strong offering across scanning types • Nice, clean UX and design • Strong offering across scanning types • Tight integration with IDEs • Strong offering across scanning types • False positive rates are better than average
Weaknesses	• GitLab's SAST offering only scans code repositories today and cannot scan compiled binaries	• Only available as a SaaS tool and cannot be deployed on-premise • Not natively integrated into merge requests or the SDLC

Feature Lineup

	GitLab	Veracode
SAST	✅	✅
DAST	✅	✅
IAST		✅
SCA: Vulnerability Scanning	✅	✅
SCA: Open Source Audit	✅	✅
Fuzz Testing	✅	

Feature Comparison

FEATURES	VERACODE	
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 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	✅	✅

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

Why GitLab?

- Product
- Solutions
- Services
- DevOps lifecycle
- DevOps tools
- Is it any good?
- Releases
- Pricing
- Get started

Resources

- All resources
- All-Remote
- Blog
- Newsletter
- Events
- Webcasts
- Topics
- Training
- Docs
- Install

Community

- Customers
- Contribute
- Partners
- Channel Partners
- Explore repositories
- Source code
- Shop
- Direction
- Contributors
- Core Team
- Hall of fame
- Community Forum

Support

- Get help
- Contact Sales
- Contact Support
- Support options
- Status
- Customers portal

Company

- About
- What is GitLab?
- Jobs
- Culture
- Team
- Press
- Analysts
- Handbook
- Security
- Contact
- Terms
- Privacy
- Trademark