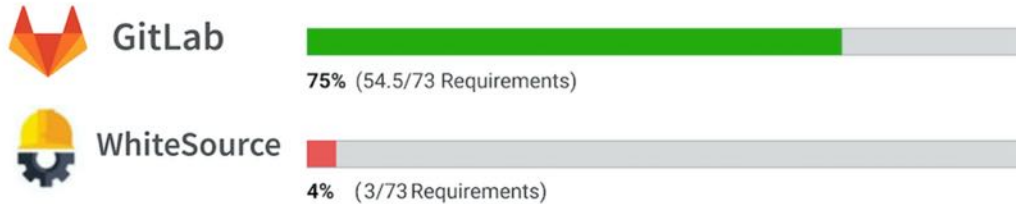


# GitLab vs whitesource

## Decision Kit



	GitLab	WhiteSource	Missing in WhiteSource
<b>Manage</b>	5.5/8		<ul style="list-style-type: none"> <li>Subgroups</li> <li>Audit Events</li> <li>Audit Reports</li> <li>Compliance Management</li> <li>Code Analytics</li> <li>DevOps Reports</li> <li>Value Stream Management</li> <li>Insights</li> </ul>
<b>Plan</b>	6/8		<ul style="list-style-type: none"> <li>Issue Tracking</li> <li>Kanban Boards</li> <li>Time Tracking</li> <li>Epics</li> <li>Roadmaps</li> <li>Service Desk</li> <li>Requirements Management</li> <li>Quality Management</li> </ul>
<b>Create</b>	7.5/8		<ul style="list-style-type: none"> <li>Source Code Management</li> <li>Code Review</li> <li>Wiki</li> <li>Static Site Editor</li> <li>Web IDE</li> <li>Live Preview</li> <li>Snippets</li> <li>Design Management</li> </ul>
<b>Verify</b>	6/8		<ul style="list-style-type: none"> <li>Continuous Integration</li> <li>Code Quality</li> <li>Code Testing and Coverage</li> <li>Load Testing</li> <li>Web Performance</li> <li>Usability Testing</li> <li>Accessibility Testing</li> <li>Merge Trains</li> </ul>
<b>Package</b>	4.5/6		<ul style="list-style-type: none"> <li>Package Registry</li> <li>Container Registry</li> <li>Helm Chart Registry</li> <li>Dependency Proxy</li> <li>Jupyter Notebooks</li> <li>Git LFS</li> <li>Dependency Firewall</li> </ul>
<b>Secure</b>	7/8	3/8	<ul style="list-style-type: none"> <li>SAST</li> <li>DAST</li> <li>Fuzz Testing</li> <li>Dependency Scanning</li> <li>Container Scanning</li> <li>License Compliance</li> <li>Secret Detection</li> <li>Vulnerability Management</li> </ul>
<b>Release</b>	7/8		<ul style="list-style-type: none"> <li>Continuous Delivery</li> <li>Pages</li> <li>Review Apps</li> <li>Advanced Deployments</li> <li>Feature Flags</li> <li>Release Orchestration</li> <li>Release Evidence</li> <li>Secrets Management</li> </ul>
<b>Configure</b>	4.5/7		<ul style="list-style-type: none"> <li>Auto DevOps</li> <li>Kubernetes Configuration</li> <li>ChatOps</li> <li>Runbooks</li> <li>Serverless</li> <li>Infrastructure as Code</li> <li>Cluster Cost Optimization</li> </ul>
<b>Monitor</b>	5/8		<ul style="list-style-type: none"> <li>Metrics</li> <li>Alert Management</li> <li>Incident Management</li> <li>Logging</li> <li>Tracing</li> <li>Error Tracking</li> <li>Product Analytics</li> <li>Synthetic Monitoring</li> </ul>
<b>Defend</b>	1.5/3		<ul style="list-style-type: none"> <li>Web Application Firewall</li> <li>Container Host Security</li> <li>Container Network Security</li> </ul>

WhiteSource scans open source code for security vulnerabilities. They claim to cover 200 programming languages. The Checkmarx dependency scanning relies on WhiteSource.

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.

## Feature Comparison

FEATURES



### Static Application Security Testing



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.



supports 18 languages

[Learn more about Static Application Security Testing](#)

### Secret Detection



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



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



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



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



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.



### Cloud Native Network Firewall



Cloud native network firewall provides container-level network micro segmentation which isolates container network communications to limit the “blast radius” of compromise to a specific container or microservice. A container-aware virtual firewall identifies valid traffic flows between app components in your cluster and limits damage by preventing attackers from moving through your environment



when they have already compromised one part of it.

[Learn more about Container Network Security](#)

### 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 is 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

Git is a trademark of Software Freedom Conservancy and our use of 'GitLab' is under license

[View page source](#) — [Edit in Web IDE](#) — [please contribute.](#)