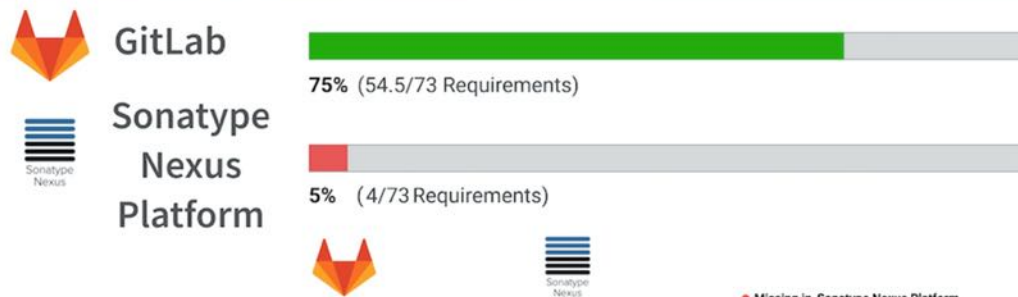


SonaType GitLab vs Nexus Platform

Decision Kit



Category	GitLab Score	GitLab Progress	Sonatype Nexus Progress	Missing in Sonatype Nexus Platform
Manage	5.5/8	<div style="width: 68.75%;"></div>	<div style="width: 0%;"></div>	<ul style="list-style-type: none"> Subgroups Audit Events Audit Reports Compliance Management Code Analytics DevOps Reports Value Stream Management Insights
Plan	6/8	<div style="width: 75%;"></div>	<div style="width: 0%;"></div>	<ul style="list-style-type: none"> Issue Tracking Kanban Boards Time Tracking Epics Roadmaps Service Desk Requirements Management Quality Management
Create	7.5/8	<div style="width: 93.75%;"></div>	<div style="width: 0%;"></div>	<ul style="list-style-type: none"> Source Code Management Code Review Wiki Static Site Editor Web IDE Live Preview Snippets Design Management
Verify	6/8	<div style="width: 75%;"></div>	<div style="width: 0%;"></div>	<ul style="list-style-type: none"> Continuous Integration Code Quality Code Testing and Coverage Load Testing Web Performance Usability Testing Accessibility Testing Merge Trains
Package	4.5/6	<div style="width: 75%;"></div>	1/7 <div style="width: 14.28%;"></div>	<ul style="list-style-type: none"> Package Registry Container Registry Helm Chart Registry Dependency Proxy Jupyter Notebooks Git LFS Dependency Firewall
Secure	7/8	<div style="width: 87.5%;"></div>	3/8 <div style="width: 37.5%;"></div>	<ul style="list-style-type: none"> SAST DAST Fuzz Testing Dependency Scanning Container Scanning License Compliance Secret Detection Vulnerability Management
Release	7/8	<div style="width: 87.5%;"></div>	<div style="width: 0%;"></div>	<ul style="list-style-type: none"> Continuous Delivery Pages Review Apps Advanced Deployments Feature Flags Release Orchestration Release Evidence Secrets Management
Configure	4.5/7	<div style="width: 64.28%;"></div>	<div style="width: 0%;"></div>	<ul style="list-style-type: none"> Auto DevOps Kubernetes Configuration ChatOps Runbooks Serverless Infrastructure as Code Cluster Cost Optimization
Monitor	5/8	<div style="width: 62.5%;"></div>	<div style="width: 0%;"></div>	<ul style="list-style-type: none"> Metrics Alert Management Incident Management Logging Tracing Error Tracking Product Analytics Synthetic Monitoring
Defend	1.5/3	<div style="width: 50%;"></div>	<div style="width: 0%;"></div>	<ul style="list-style-type: none"> Web Application Firewall Container Host Security Container Network Security

Sonatype Nexus Platform is comprised of multiple products which contribute to the Sonatype Nexus security capabilities. Those products are Nexus Lifecycle, Nexus Auditor, Nexus Firewall, and Nexus Repository Pro, and the Nexus Intelligence service. In the application security space, Sonatype Nexus scans open source components for security vulnerabilities, scans containers and offers license management. Fortify relies on Sonatype for dependency scanning.

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.

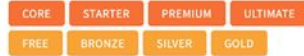
For packaging deployments, both Sonatype and GitLab offer container registry, but Sonatype also offers a full binary repository in the form of Nexus Repository (available in both OSS and Pro).

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.



[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.*



many cases and more, GitLab does not get over the feature.

Cloud Native Network Firewall

- CORE
- STARTER
- PREMIUM
- ULTIMATE
- FREE
- BRONZE
- SILVER
- GOLD

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

