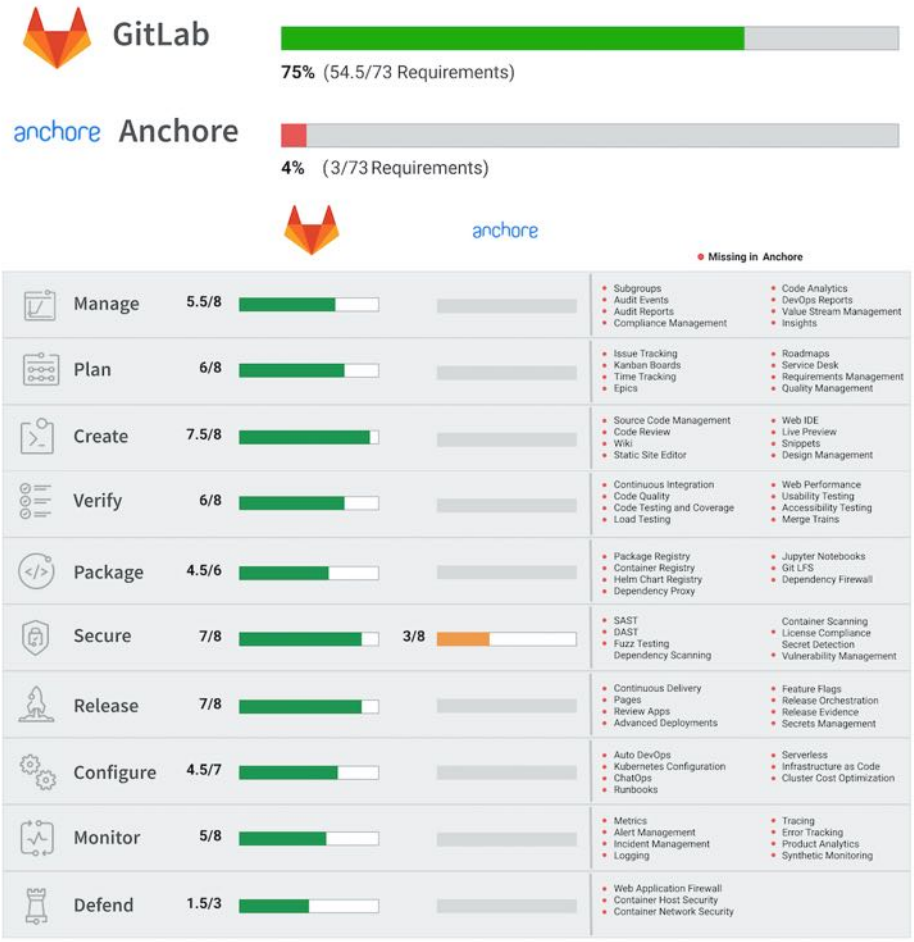
GitLab vs Anchore

Decision Kit



Summary

Anchore is a company that offers security scanning for Docker containers, Docker container registries, and Kubernetes clusters. They offer an Open Source, Enterprise, and Federal version of their products. They leverage public vulnerability feeds to scan customers' environments for vulnerabilities and alert them so end users can take action.

Comparison to GitLab

Although Anchore does software composition analysis well, they do very little beyond that narrow scope. Comparatively, GitLab provides a superior experience for ALL types of security scanning - not only container scanning, but also SAST, DAST, Fuzz Testing, and others. This approach maximizes the kinds of vulnerabilities that can be detected while only incurring the maintenance costs of a single tool.

Anchore leverages publicly-available vulnerability feeds to identify their vulnerabilities. GitLab does this as well; however, GitLab is also a CVE Numbering Authority, which means that security researchers can work directly with GitLab on any security issues they find. GitLab's commitment to leveraging the latest vulnerability feeds is also publicly visible to customers at advisories.gitlab.com.

Finally, GitLab provides a superior experience for developers in viewing, correcting, and responding to vulnerabilities. Because GitLab's scanning capabilities are integrated with the rest of GitLab, the vulnerabilities appear as part of the developer's regular workflow, inline within their MRs. This visibility is critical to be able to effectively shift security left. With Anchore, developers will need to look at an external tool to see the details about their vulnerabilities, making them much less likely to correct them before the code goes to production.

Anchore can be complementary to GitLab if users have already bought both. GitLab supports integration with tools that customers are already using and plays well with others.

Software Composition Analysis (SCA)

Strengths and Weaknesses

	GitLab	Anchore
Strengths	• Integrated security as part of DevOps workflow for all developers • High-quality container security by leveraging all the latest feeds for vulnerabilities • Supports on-premise deployments including disconnected, offline, or air-gapped environments • Security leadership by being a CVE Numbering Authority and a recognized in the Gartner AST magic quadrant • End-to-end DevOps offering from SCM to CI to CD to Security and more	• Single-focused, purpose built container scanning product • Can work with many CI/CD providers (e.g. GitHub, GitLab, BitBucket)
Weaknesses	• Pricing requires buying all of GitLab Ultimate, not just Container Scanning	• Narrow product offering only focused on one type of scanning • It is difficult to justify the cost of maintaining an entire security tool when the tool addresses such limited scope (SCA only)

Feature Lineup

	GitLab	Anchore
Vulnerability Scanning	✅	✅
Secrets and Passwords	✅	✅
Open Source & Third Party Package Audit	✅	✅
Air-gapped Support	✅	✅
Security results shown to developers as part of their daily work	✅	

Feature Comparison

FEATURES	anchore	
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	✓	✓

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