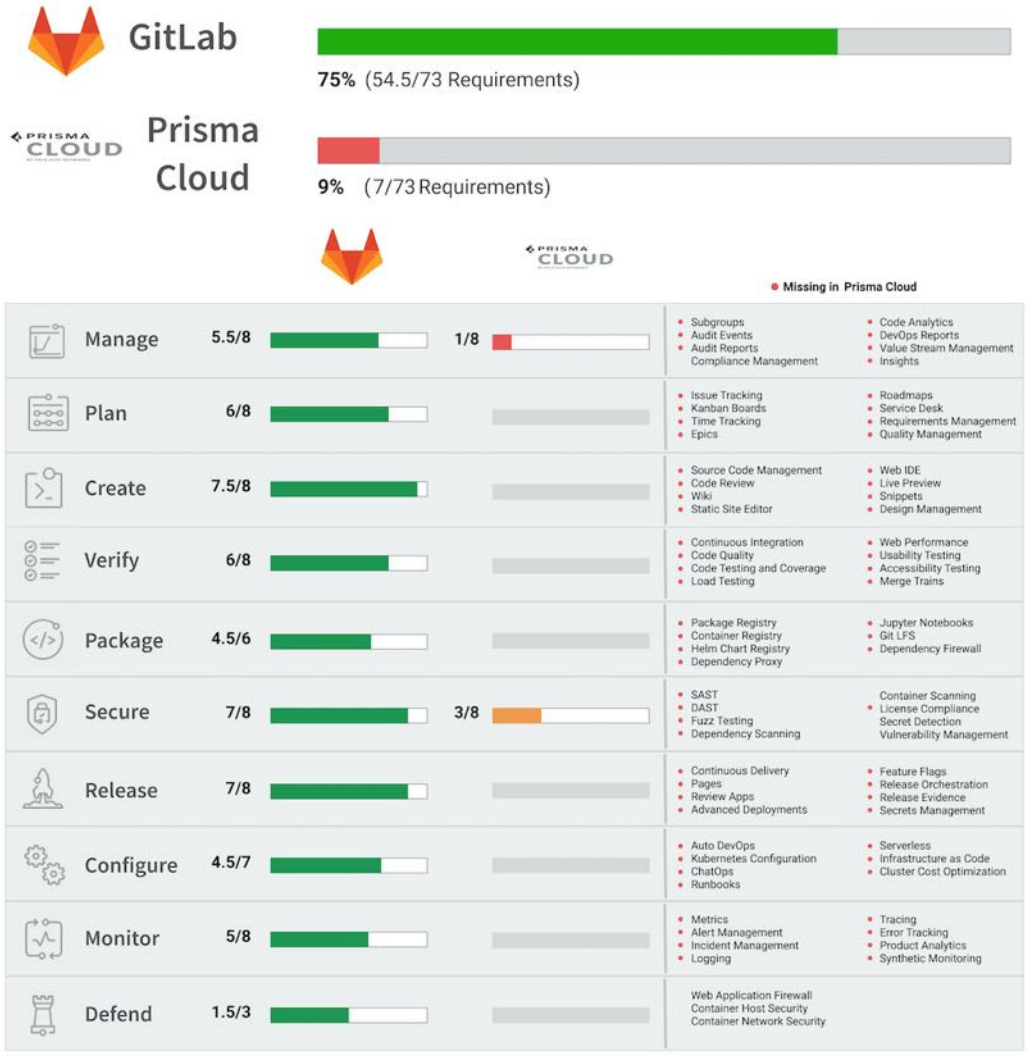
GitLab vs Prisma Cloud

Decision Kit



Summary

Twistlock was recently acquired by Palo Alto and was subsequently rebranded as Prisma Cloud. Prisma Cloud plays in several categories that overlap with GitLab. Pricing is based on the number of "workload" (aka. pods) that are protected.

Palo Alto's Prisma Cloud product provides lifecycle security for containerized environments, "from pipeline to perimeter". Prisma Cloud capabilities include runtime defense, vulnerability management, cloud native firewalls, and pre-built compliance templates for HIPAA, PCI, GDPR, and NIST SP 800-190. It can be integrated into your CI/CD pipeline. Automated and custom policies can block builds or deployments based on vulnerabilities or compliance requirements. Runtime capabilities were recently expanded from only containerized applications to include VMs.

Comparison to GitLab

Prisma Cloud's runtime and container security features are robust, but they do not offer the breadth of GitLab's security scans. 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. Prisma Cloud is also expensive, while much of the current feature set that GitLab provides is available for free. Additionally, the heavy operational maintenance burden of Prisma Cloud further adds to the cost. If what GitLab provides today can be considered 'good enough', then customers can potentially save a huge amount of money.

Security Scanning

Prisma Cloud is a decent choice for customers that only need basic vulnerability scanning; however, their vulnerability management tool only intakes data from a single, limited source: known CVEs. This leaves them blind to other vulnerabilities that may be identified through SAST or DAST scans. For customers to properly secure their applications, they should consider a solution that includes good SAST and DAST scanners. Rather than using separate scanners to meet their needs, it will be much simpler and easier to use GitLab, which both has a wide range of scanning capabilities, a native integration with SCM, and has been recognized in the Gartner Magic Quadrant for Application Security Testing (AST).

Strengths and Weaknesses

	GitLab	Prisma Cloud
Strengths	• Integrated security as part of DevOps workflow for all developers • High-quality container security by leveraging all the latest feeds for vulnerabilities • Security leadership by being a CVE Numbering Authority • End-to-end DevOps offering from SCM to CI to CD to Security and more	• Provides a basic analysis of installed packages vs. known CVEs • Nice, clean UX and design
Weaknesses	• Requires users to use GitLab for CI if they are not already	• Does not provide a full suite of code scanning to adequately detect all vulnerabilities - no SAST or DAST • Shifting left and integrating with SCM tools requires an integration to be built with their APIs and does not exist natively

Feature Lineup

	GitLab	Prisma Cloud
SAST	✅	
DAST	✅	
SCA: Vulnerability Scanning	✅	✅
SCA: Open Source Audit	✅	
Fuzz Testing	✅	

Vulnerability Management

Additionally, using Prima Cloud requires customers to integrate a separate product into their CI/CD pipeline jobs. Customers can save time and money by instead using GitLab's built-in vulnerability management capabilities that come available out-of-the-box. For customers who do decide to use Prisma Cloud, it is possible to feed their scan results into GitLab and combine them with the results from other GitLab scans.

Strengths and Weaknesses

	GitLab	Prisma Cloud
Strengths	• One tool - vulnerability management is integrated out-of-the-box • Visualizes data from all of GitLab's scanning engines, including DAST, SAST, and SCA	• Capable of enforcing policy rules and preventing vulnerable code from running • Good visualization of a complex risk analysis • Capable of showing CVE severity together with the container's actual exposure to the specific attack
Weaknesses	• Although the roadmap is robust, current functionality is new and lacks features • Risk assessment capabilities do not exist and priorities do not take into context the configuration of the container, which could mitigate some vulnerabilities	• Lacks good scanners to identify vulnerabilities • Not natively integrated with SCM tools - an API is available but the integration has to be built into CI/CD • Limited to containerized applications

Feature Lineup

	GitLab	Prisma Cloud
Vulnerability Assessment	✅	limited
Risk Assessment		✅
Vulnerability Prioritization	limited	limited

Vulnerability Prioritization	limited	limited

Container Security

As GitLab's container security capabilities are relatively new, Prisma Cloud has a much more robust feature/functionality set than GitLab in securing containerized workloads. Additionally, Prisma Cloud is capable of protecting serverless code as well as virtual machines. GitLab's container security roadmap is robust and the feature set is maturing quickly. Additionally, all of the base security capabilities are available in GitLab's free, Core tier.

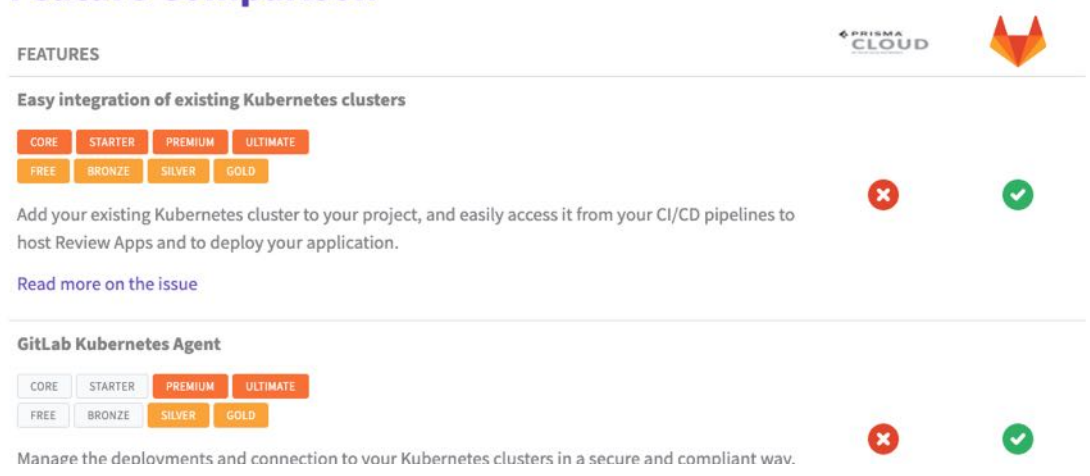
Strengths and Weaknesses

	GitLab	Prisma Cloud
Strengths	• Current functionality provides a respectable baseline of security (Web application firewall, container Network Policies, container host monitoring) • Base security capabilities are currently available in the free Core tier	• Extensive set of features and capabilities • "Radar" capability gives a wow factor in visualizing the network • Protection for VMs, containers, and serverless code
Weaknesses	• Although the GitLab roadmap is robust, current functionality is new and lacks features • Current capabilities are supported in containerized environments only	• Pricing model can get expensive fast with lots of containers • Behind the nice UX, the solution is hard to manage and can require a lot of time from a dedicated team

Feature Lineup

	GitLab	Prisma Cloud
Network Firewall	✅	
Machine Learning		✅
Active Vulnerability Scanning (of an application running in production)		✅
Malware Scanning		✅
Exploit Protection		✅
File Integrity Monitoring	✅	✅
Application/Binary Allow Listing	✅	✅
Log Monitoring	✅	✅
Compliance		✅
Identity and Access Management		✅
Active Response / Blocking	✅	✅
Virtual machine Support		✅
Kubernetes/Container Support	✅	✅
Serverless Support		✅

Feature Comparison



driven by code.

Read more on the issue

Custom header and footer system message in web and email

CORE STARTER PREMIUM ULTIMATE
FREE BRONZE SILVER GOLD

Include custom header and footer system messages throughout GitLab and in emails.

Read about Custom header and footer system message in web and email

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.

supports 18 languages

Learn more about Static Application Security Testing

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.

Vulnerability Management

CORE STARTER PREMIUM ULTIMATE
FREE BRONZE SILVER GOLD

GitLab's vulnerability management is about ensuring assets and applications are scanned for vulnerabilities. It also includes the processes to record, manage, and mitigate those vulnerabilities.

Vulnerability management helps identify meaningful sets of vulnerabilities, in both your assets and application code, that can be mitigated, managed, and acted upon by your whole team—not just the

security organization. It also provides a unified interface to the systems teams are already using for managing results from the ~"devops::secure" stage so there is always a single source of truth and single place for managing security results.

Learn more about Vulnerability Management

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

Container Host Monitoring and Blocking

CORE STARTER PREMIUM ULTIMATE
FREE BRONZE SILVER GOLD

"With Container Host Monitoring, you can monitor running containers for malicious or unusual activity. This includes process starts, file changes, or opened network ports. You can also block or prevent these activities from occurring."

Learn more about Container Host Monitoring and Blocking

Automated Accessibility scanning of Review Apps

CORE STARTER PREMIUM ULTIMATE
FREE BRONZE SILVER GOLD

Performing accessibility testing is important in order to ensure you're serving all the users who use your products. In GitLab you can generate Accessibility reports automatically prior to merging into master.

Learn more about Autoamted Accessibility scanning

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

Compliance Dashboard

CORE STARTER PREMIUM ULTIMATE
FREE BRONZE SILVER GOLD

Compliance management within GitLab is easier with an aggregate view of all project activity. View the compliance status of your group in a fast, simple way. Easily spot when projects are out of compliance and take informed actions to remediate any issues.

Learn more about Compliance Dashboard

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