GitLab Duo

Your AI evaluation toolkit:

How to select the right AI solution for software development

GitLab

For many developers and DevSecOps teams, AI has become critical to the software development process. In fact, according to GitLab's Global DevSecOps Report, 60% of respondents believe it to be essential for them to implement AI in their software development processes in order to avoid being left behind.

Despite the need for AI tools, there are concerns around adopting AI at such a rapid pace – 55% of respondents shared that introducing AI into the software development lifecycle (SDLC) is risky. It makes sense – AI can be risky when it isn't properly implemented.

These concerns are valid, but careful planning and choosing the right vendor can reduce many of the risks associated with AI. In this guide, we'll help you navigate choosing the right AI solution for your software development by equipping you with best practices and the best questions to ask when going through the vendor selection process.

The top 9 questions to ask potential AI solution vendors

These questions are designed specifically for AI tools for software development. While you should prepare additional questions specific to your business, team, and its needs, use these questions as a jumping off point for your vendor selection process.

1 How many LLMs does your AI solution provider support?

Each large language model (LLM) has its own focus, customized to specific industries and applications. The use of multiple LLMs from different vendors means the AI solution is using the best LLM for each use case. By diversifying the LLMs being utilized, the business is able to enhance the performance, efficiency, and innovation of their AI tool.

Multiple LLMs have the added benefit of reducing the likelihood of service disruptions. If a company relies on a single LLM, the chance of disruption, data privacy breach, and biases increase.

- **What to look for:** Multiple LLMs from multiple vendors
- **Red flag:** A single LLM

Get a behind-the-scenes look at how GitLab evaluates LLMs and matches them to each use case.

2 How does the AI solution provider use customer data?

A company's proprietary data is one of its most valuable assets, allowing a business to make informed decisions that power its products and services. Many AI models leverage company data because high-quality data is necessary to AI model quality and performance, but when AI models leverage your data they put your valuable information at risk.

If both you and your competitors use the AI model, the model could provide recommendations from your proprietary data that benefit your competitors.

Additionally, the data stored within the model can be accessed through data harvesting. If users repeatedly query APIs or product features that rely on proprietary data, users can access meaningful amounts of your company's data.

What to look for: A privacy-first policy

"Privacy-first" is a methodology that prioritizes data privacy from both a technical standpoint and business perspective. This policy minimizes the amount of data collected from customers, is extremely transparent with how data is collected, and safeguards customer data from security breaches.

Red flag: A lack of transparency around data usage

It's up to you and your business whether you're comfortable with AI models leveraging your data. However, if a company is vague or unclear with how they plan to use your company's data, that should be a dealbreaker.

GitLab's privacy-first policy

"Transparency is a core value at GitLab, and we take a transparency- and privacy-first approach to building our AI features to help ensure that our customers' valuable intellectual property is protected. Accordingly, we've launched our AI Transparency Center to help GitLab's customers, community, and team members better understand the ways in which GitLab upholds ethics and transparency in our AI-powered features."

Robin Schulman,
Chief Legal Officer, Gitlab

Explore GitLab's AI Transparency Center >

The top obstacle to AI usage is concerns around privacy and data security.

The Global DevSecOps Report

3 Do I own the input of what I entered into the AI solution and the output generated by the AI solution?

While it's helpful to know that the AI solution does not use customer data to train its model, it's equally important that you own the data that you are inputting and receiving.

Your intellectual property is vital to your organization, especially in software development, which makes your AI queries and the corresponding AI suggestions valuable information. Ask potential vendors about their policies on data ownership and how they track the usage of their AI systems.

- **What to look for:** Ownership of your AI queries and responses
- **Red flags:** All AI-usage data is owned by the AI provider

4 Does the AI solution support multiple deployment options?

Just as multiple LLMs are important to the effectiveness of the AI solution, multiple deployment options provide flexibility, scalability, and security to the development processes.

Support for multiple deployment options, such as self-managed, multitenant on the cloud, single-tenant on the cloud, give developers the flexibility they need to select the best deployment method for each use case.

- **What to look for:** Multiple deployment options that are cloud-agnostic
- **Red flag:** Only supports one deployment option or requires use of one cloud platform

GitLab

5 Does the AI solution offer features that support all DevSecOps teams?

AI-supported code creation has been a common use case for DevSecOps teams, and while valuable, this feature only scratches the surface of what's possible with AI. It also makes up only a fraction of a developer's day-to-day workload.

To accelerate your processes across the SDLC, look for capabilities that support the entire DevSecOps lifecycle such as **summarization tools**, **vulnerability explanation and resolutions**, and **root cause analysis**.

- **What to look for:** Comprehensive AI features across the SDLC
- **Red flags:** Offers only code creation or limited capabilities

The #1 AI use case is code creation
The Global DevSecOps Report

<25%
of a developer's time is spent writing new code
The Global DevSecOps Report

Cube leverages GitLab Duo across the entire SDLC

"We went with GitLab Duo because it has features, like Code Suggestions, test generation, and summarizations, that immediately were able to help us become more efficient. We wanted to use a whole package of AI features on one platform."

Mans Booijink,
Operations Manager, Cube

Challenge → Cube's DevSecOps team members wanted to save time on projects through AI-supported code creation and chat assistant.

Solution → Cube turned to GitLab Duo to increase its efficiency and speed in creating secure software.

Results → Cube now saves 40 hours per week with 50% faster release cycles and 50% faster vulnerability detection.

Read the full customer story ›

6 Does your AI solution enhance the security detection processes within the SDLC?

When AI solutions are integrated into your SDLC, they should streamline your security detection and resolution processes and not add to the complexity of securing your systems.

Consider AI tools that are built into your DevSecOps platform. This allows you to streamline and enhance your security and compliance processes across all environments, and automatically incorporate security scanning tools such as **static application security testing (SAST)** and **dynamic application security testing (DAST)**.

Ultimately, it's up to you whether you'd like an AI solution that integrates with your SDLC or is built into your DevSecOps platform. But, there are advantages to a built-in solution.

GitLab's DevSecOps report found that 74% of respondents whose organizations are currently using AI for software development said they wanted to consolidate their toolchain compared to the 57% that are not using AI.

By choosing an AI solution that is built directly into your DevSecOps platform, you can reduce context switching and the complexity of your toolchain.

- **What to look for:** Fully supported security solutions
- **Red flag:** A lack of security infrastructure

7 Does your solution offer reporting to measure the success of my programs and the impact of the tool?

Understanding how AI is impacting your day-to-day operations and workload can help prove AI's value. Solutions that offer **built-in AI impact analysis** are ideal to see the value and results you're receiving from AI adoption.

While some solutions offer third party tools to measure AI's effectiveness, this often leads to greater toolchain complexity and additional context switching for developers.

- **What to look for:** Built-in AI impact analytics
- **Red flags:** No analytics or solutions that offer analytics in separate tools

GitLab

8 Does your AI solution offer training to support my team?

Two of the top challenges to AI adoption revolve around the training and understanding of AI tools. Like any new tool, AI has a learning curve and requires education to use it to its full potential.

Ask vendors what support they provide to teams through documentation, courses, and training services.

- **What to look for:** Comprehensive training packages and documentation
- **Red flag:** Limited documentation and training options for customers

The top two and three obstacles that respondents experienced when using AI are:

31%
A lack of the appropriate skill set to employ AI or interpret AI output

30%
A lack of knowledge about AI

9 What ongoing maintenance and support is in place for your AI solutions?

AI technology is rapidly evolving. A company's AI solution may be cutting edge today, but could easily be outpaced by competitors if they are not frequently updating the models and underlying technology. Ask AI vendors about their cadence of updates, release cycles, or changelog to get a better understanding of the vendor's pace of innovation.

- **What to look for:** Regular updates, upgrades, and proactive monitoring
- **Red flag:** Inconsistent updates of their changelog or version releases

Best practices for AI solution vendor evaluation

When evaluating an AI solution for your software development processes, the questions above will help guide your conversations, but there are a few tried-and-true best practices in mind.

Understand what problems you're trying to solve

Knowing the top problems you're solving for can help you determine what features are absolutely necessary in your vendor selection process.

Prioritize transparency and documentation

Avoid solutions that are not transparent or clear about their policies. If the responses are vague, the companies may not have policies in place to protect your company's data or security.

Request case studies and references

Ask for success stories and references. This can help you see how similar companies leverage the AI tools and whether it would be a good fit for your company.

Review potential ROI

By reviewing case studies and understanding the potential impact of AI on metrics such as time-savings or vulnerability reduction, you can estimate the ROI of the solution. This is also where AI impact analytics provide valuable insights. Once you have implemented the AI tool, you can determine the true value-add of the tool and whether it is worth keeping.

Start small

Test out a pilot program before committing to an AI solution across your SDLC. This can help you determine whether or not the solution is a good fit for your business before incorporating AI into every team member's day-to-day workflow.

Evaluate GitLab Duo as your AI solution vendor

As part of your AI evaluation process, explore GitLab Duo. GitLab recognizes that developers, operations, and security teams need support beyond code creation, and was created to enable DevSecOps teams to create secure code faster at every stage of the SDLC.

GitLab Duo prioritizes your security, privacy, and functions seamlessly within your GitLab DevSecOps platform. It offers:

- Multiple LLMs to support a variety of use cases
- A privacy-first approach
- Customers ownership of AI inputs and outputs
- Multiple deployment options
- Built-in analytics
- Extensive documentation and support options

Add GitLab to your shortlist, and explore GitLab Duo today.