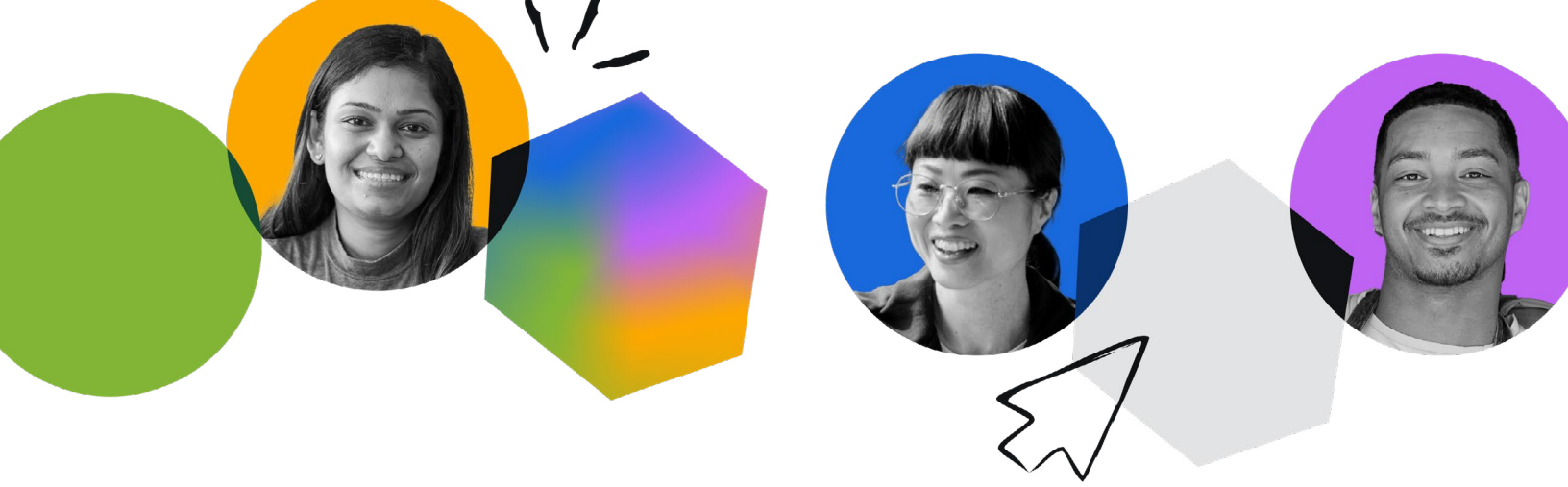


ATLASSIAN

Harness the potential of Atlassian AI with the confidence that your data is protected

Artificial intelligence (AI) capabilities are changing the way teams work together at an unprecedented rate. Teams can now find information faster, accelerate decisions across disparate teams, and build better customer solutions with the power of AI. Over the next three years, **92% of companies plan to increase their AI investments**. The fast pace of AI adoption means organizations need to take a proactive approach to addressing security and maintaining compliance with AI. To do this effectively, companies should build a trusted approach to using AI that is rooted in a multi-layer strategy.

As you prepare to use AI across your organization, consider the key principles you use today when evaluating your other trusted cloud providers. Many industry-standard security, privacy, and compliance principles offer a strong, multi-step foundation for evaluating and implementing AI solutions. In this guide, we'll walk through some key considerations to help you build an understanding of Atlassian's approach to trust, how it applies Atlassian Rovo, and the controls you can use to enable AI-powered features in Atlassian cloud confidently.

Prioritize organization-wide visibility

You can't protect what you can't see. Empower your admins and security teams with the visibility needed to effectively manage AI permissions and activity.

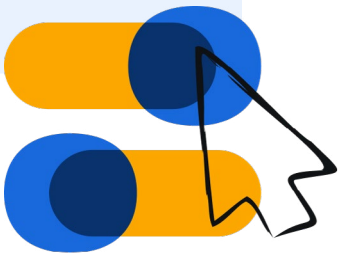
Gaining visibility into the information accessible to your users is crucial for effectively minimizing risk and safeguarding your data. AI is best suited for scenarios where organizations can establish strong data connections across departments. Providing better context to AI solutions can significantly boost collaboration among your teams.
This improvement facilitates quicker insights across various projects, ultimately resulting in more effective outcomes.

To prepare your organization for AI, it is important to review and confirm that your data is accurately identified and classified. Understanding where your data is, who has access to it, and how much of it is considered sensitive is the first step your organization should take as you look to enable AI.

These best practices apply to all software vendors you may be evaluating. When it comes to increasing visibility within your Atlassian portfolio specifically, there are several dashboards available to review and maintain visibility over your Atlassian cloud environment.

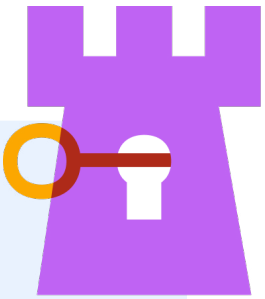
Turning best practices into action:

- The **organization insights dashboard** in Atlassian Administration enables you to view daily and monthly active users across the Jira, Jira Service Management, and Confluence cloud products that are linked to your organization.
- **Mission Control**, available in Confluence, allows you to easily see who has administrative and external access, the number of spaces, feature usage, and content that is most frequently consumed on your site.
- The **AI insights tab**, available in the organization insights dashboard, offers greater visibility into how AI-powered Rovo features are being used over time. You can also use these insights to identify usage gaps and connect more teams with AI capabilities.



Secure by design with privacy and compliance in mind

AI solutions should be developed with the same level of rigor expected for your other cloud products to ensure they meet your organization's security, privacy, and compliance requirements.



As you evaluate AI solutions, understand your organization's requirements for onboarding new cloud products. Most organizations have established core trust requirements for AI solutions that account for security, privacy, and compliance. As AI continues to evolve rapidly, many cloud service providers have aligned the development of their AI solutions to responsible technology or ethical AI principles. Reviewing these principles can help you better understand how each organization approaches the security and privacy design of their AI solutions.

Investigate how your data will be used, stored, and shared. Your solution provider should be transparent about these things and offer assurances on how your data will be handled.

Atlassian's AI approach is rooted in our Responsible Technology Principles.

Atlassian's approach to protecting your data:

- ☑ The policies and terms incorporated by reference in the Atlassian Customer Agreement, including the Privacy Policy, Acceptable Use Policy, Data Processing Addendum, Product-Specific Terms, govern your use of Rovo.
- ☑ We use both Atlassian-hosted (Mixtral, Phi, and Llama-3) and third-party LLMs, including OpenAI, Anthropic, and Gemini. The LLM providers we use do not retain your inputs and outputs, or use them to improve their services. Please refer to our list of data sub-processors for more information on our external LLM providers.
- ☑ Rovo adheres to the same security standards and practices that govern all of our products and platform. We also offer end-to-end encryption at rest and in transit to ensure your data stays protected.
- ☑ Rovo respects the permissions of any third-party products you've connected.
- ☑ Your inputs and outputs are used only to serve and improve your experience. They are not used to train LLM models across customers.
- ☑ Rovo maintains compliance with regulatory requirements, including SOC 2 and ISO27001.
- ☑ Atlassian publishes detailed documentation for Rovo capabilities on our transparency page.

Control over your data

Set company-wide standards that can help you take control of where your data is, who has access, and how they can use it.

Now that you've assessed your organization and have an understanding of your users and data, it is time to evaluate your permissions and controls. To minimize the risk of your users seeing content they shouldn't, we highly recommend auditing your existing user permissions and content policies. When your organization identifies certain types of data as sensitive, you should implement and uphold the appropriate controls. Setting data access controls reduces overall risk to your organization and ensures that only authorized users who require access to this data can do so.

When using Rovo, you can set policies that help give AI access to the context and data needed to supercharge collaboration with assurance that your permissions and data sensitivity levels are respected.

Controls and settings that help you manage Rovo with confidence:

- ☑ Rovo respects the permissions you've set in your Atlassian products and third-party connectors, so that users only see the data they have access to.
- ☑ Atlassian cloud offers a **delegated admin experience** that enables you to set permissions at multiple levels: org, site, and product.
- ☑ You have control to **enable or disable AI** at any time. Simply visit Atlassian Administration to manage your settings at the product level.
- ☑ Consistently review content within your organization and confirm that access to sensitive information remains restricted across your organization.
- ☑ Keep your Rovo data in the region of your choice with data residency support for **in-scope product data** to meet your regional and regulatory requirements.

Unleash AI potential with trust

Taking a trusted approach to rolling out AI doesn't have to slow down innovation across your organization. With Rovo, you can bring the power of AI into Atlassian's cloud products, securely.

- ☑ Take the first step in understanding your organization's current environment and trust requirements.
- ☑ Set policies and controls that give you deeper visibility into how your teams are using AI. You can use those insights to empower your teams to embrace AI for deeper collaboration and improved efficiency.
- ☑ Continually evaluate how your organization uses Rovo to ensure the permissions and policies you've implemented continue to meet your security and compliance requirements.

Have more questions about Atlassian's approach to trust for AI?

Visit the Atlassian Trust Center

ATLASSIAN