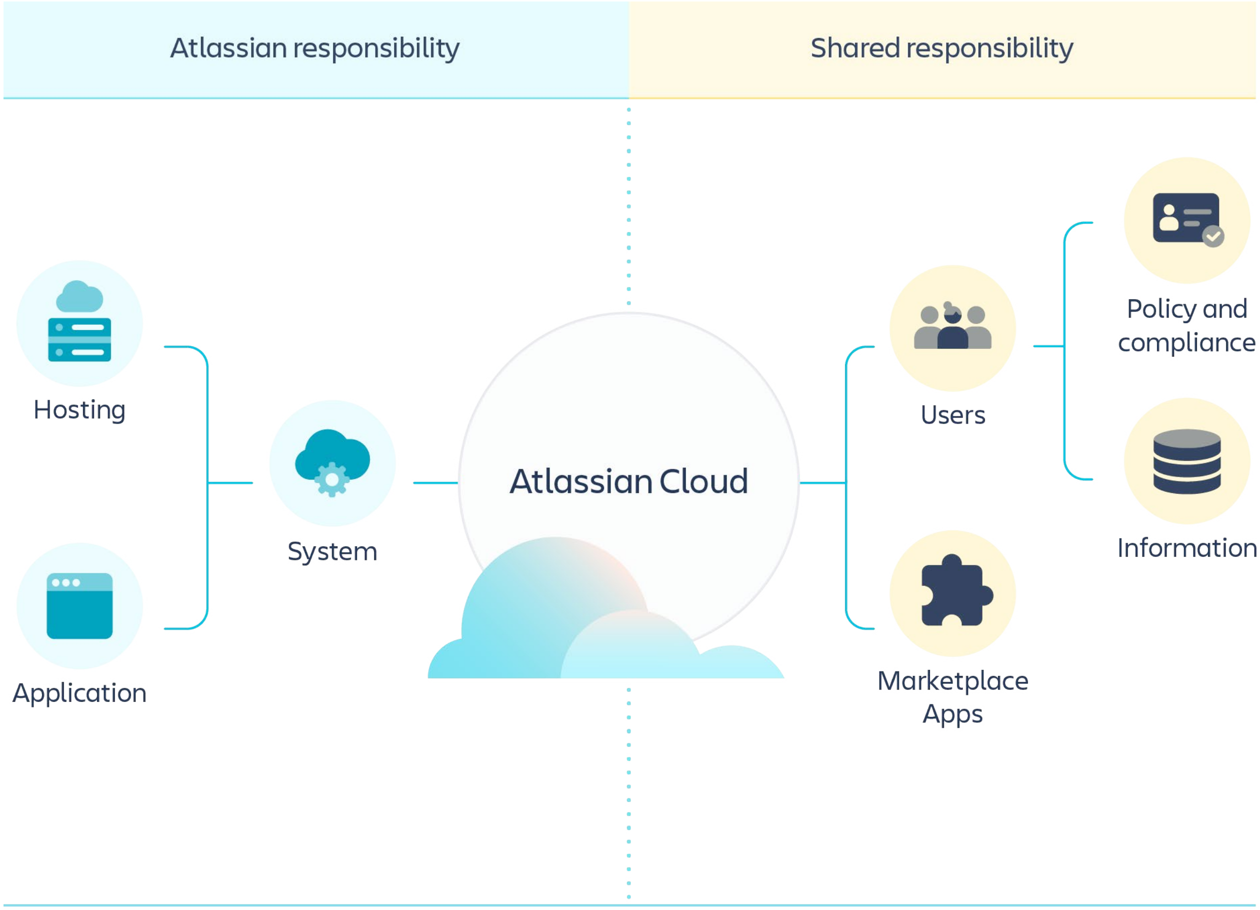
ATLASSIAN

Atlassian Cloud security shared responsibilities

Our partnership in the cloud

It is Atlassian's mission to unlock the potential of every team. As our partner, we want to emphasize that *we are on the same team and are here to support your needs across our platform.*

We know you trust Atlassian to provide products and solutions to customers across industries, geographies, and regulatory obligations. We live by Atlassian's **company values** and aspire to be an open company that puts customers' needs at the center of everything we do. As we advance our Cloud offerings, we understandably receive questions from our customers as to how Atlassian approaches the protection and confidentiality of our customer's data as a cloud service provider. The responsibilities detailed in this paper broadly apply across our platform.



The shared responsibilities model

In Cloud, Atlassian focuses on the security, compliance, and reliability of the applications, the systems they run on, and the environment those systems are hosted within. We ensure your systems and environments are compliant with relevant standards, including **ISO27001**, **SOC2**, **GDPR**, and many others that live with our **Trust Center**.

You, our customers, manage the data within your accounts, the users and user accounts accessing your data, and control which Marketplace Apps (formerly called “add-ons”) you install and trust. When using our applications, you are responsible for ensuring your organization is using our products in a compliant way.

In this paper, we will discuss the actions we take to protect your data, and how Atlassian can best help you as we embark together.

Our guiding principles

Atlassian is well known for our values, and those values genuinely influence everything we do – including our approach to shared security responsibilities in Cloud. In practice, our values have led us to the following guiding principles about shared responsibility:

One team

We're on the same team, and our customers are the motivating factor of everything we do. We strive to support you and meet your requirements along the way.

Trust in transparency

We know that honesty and integrity are key to any relationship. We will be as transparent as possible about the way we do things.

Prioritize platform reliability

We've built our platform and infrastructure to support your organization today, as well as in the future. It is our responsibility to ensure our products are resilient and available for you when you need them and as you scale.

Defense in depth

We implement layered controls and make sure all parties who are a part of the Atlassian ecosystem are rowing in the same direction.

The pillars of Trust at Atlassian

Trust in Cloud is our top priority, and with Atlassian Cloud, we take on responsibilities of hosting and maintaining infrastructure your products run on. This is a foundational layer of Trust, and each of the subsequent pillars (reliability, security, privacy, and compliance) builds upon our **infrastructure and architecture practices**. We believe in being transparent about the practices and processes we use with our Cloud products, so you are informed and feel secure as our partner.

1. Reliability

Our Cloud is built to support organizations by providing a reliable platform that can dynamically scale as you grow. We approach this responsibility by focusing our infrastructure, platform, and product development on resiliency, scale, and performance.

We have disaster recovery and business continuity programs in place to ensure that our products can withstand outages, as well as hold ourselves accountable by instituting SLAs and publishing our service availability status. You can review our in-depth approach at **Reliability at Atlassian**.

2. Security

We design our Cloud products, infrastructure, and processes with security in mind. We take the responsibility of protecting your organization's data seriously, and our approach to security is based around our responsibility to be an industry-leader in Cloud and product security.

The **security section** of our Trust Center outlines our detailed approach and proactive security protocols.

3. Privacy

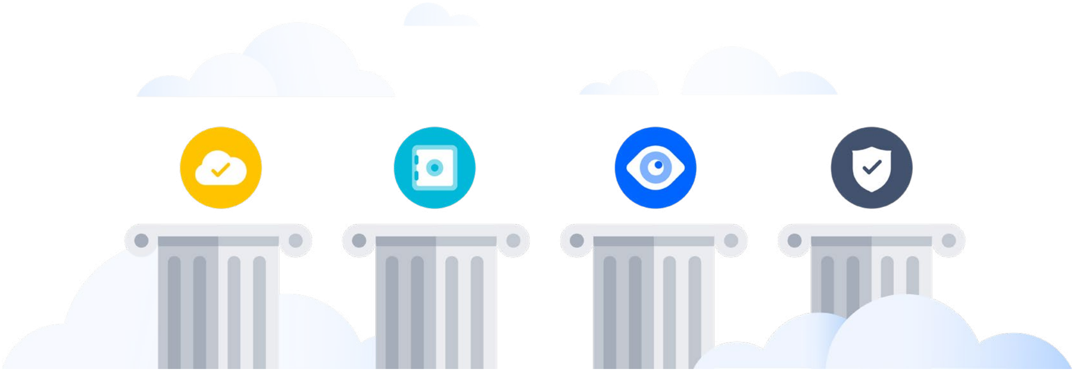
You own your data, and we're committed to protecting the privacy of your data. Our **Privacy Policy** explains what information we collect about you and why, what we do with that information, how we share it, and how we handle the content you place in our products and services. Our **Guidelines for Law Enforcement Requests** outlines our process for how we receive, scrutinize, and respond to government requests for customer information.

This information, and more, is always available within the **privacy section** of the Trust Center.

4. Compliance

A critical aspect of Cloud migrations is validating compliance and entrusting the right Cloud partner for your organization. We are actively growing our compliance certifications across geographies and industries in order to meet your needs. We strive to adhere to the widely accepted compliance standards and actively monitor evolving regulations with a proactive approach. We test our operations, environment and controls using independent, third-party advisors.

Our **compliance resource center** within the Trust Center provides comprehensive information about our Compliance Program and our growing list of certifications.



Decisions, decisions

The decisions you make about how you set up our products significantly influence the way security is implemented.

⇄ Key decisions include:

Domain verification and centralized management

You can verify one or multiple domains to prove that you or your organization own those domains. Domain verification and user claim allows your organization to centrally manage all its employees' Atlassian accounts and apply authentication policies (including password requirements, multi-factor authentication, and SAML). After verifying your domain, you claim all users with existing Atlassian accounts under that domain. Anyone signing up for a new Atlassian account with that domain will see that they are getting a managed account.

Granting access to *your data*

Our products are designed to enable collaboration, which requires access. But you do need to be careful about granting permissions to access your data to other users, and to Marketplace Apps. Once you grant such permissions, we will *not* be able to prevent those users from taking the actions allowed under those permissions, even if you don't approve of those actions. In some products you have the ability to grant public anonymous access to your data. If you permit such access, you may not be able to prevent that information being copied or further distributed.

Centralized user access management

Our customers are strongly encouraged to use **Atlassian Access** for centralized administration and enhanced security across all Atlassian products they use (including use of enforced 2FA and single sign-on).

Doing our part

Atlassian's Trust Management Program takes the security requirements of our customers into consideration, along with industry standards and expectations, and arrives at a set of requirements unique for our company.

Our trust strategy is built around the following themes:

- Continually enhancing security in our applications, our platform, and our environment to provide a compelling standard in our products and services – commonly known as continuous improvement.
- Being open and transparent about our programs, processes, and metrics. This includes sharing our journey and encouraging other cloud providers to do the same, and setting new standards for customers.
- Identifying present and future security threats to Atlassian and its customers, and limiting the impact and duration of security incidents.

Details of our initiatives are provided on the Trust Center, where you can download or request Atlassian's certification reports for ISO 27001 and SOC2, and can follow a link to review our Cloud Security Alliance (CSA) STAR questionnaire. You can also view details of the Atlassian Controls Framework we have developed to bring together the security requirements of seven international standards, which underpins our approach to security and compliance.

The CSA STAR entry includes answers to more than 300 questions included in the Consensus Assessments Initiative Questionnaire (CAIQ). As with this paper, our Atlassian CAIQ entry covers our Jira, Confluence, Bitbucket, Halp, Jira Align, Opsgenie, Statuspage, and Trello, and we will add entries for other products as needed. Those controls are then verified via various audits associated with SOC2, ISO 27001, and PCI DSS.

Shared responsibility

In the security model shown on the first page, four areas are identified as a shared responsibility.

Policy and Compliance: The approach meets your business needs and is operated in accordance with industry, regulatory, and legislative compliance obligations

Users: The creation and management of user accounts

Information: The content you store within Cloud

Marketplace Apps: Third party services which you give access to your information and the ability to integrate with Atlassian products

Policy and compliance

What Atlassian does

- ☑ Consider the risk profile of our customers when assessing the need for security controls
- ☑ Have a comprehensive security risk management program in place and effectively implement the controls detailed in our CSA STAR response
- ☑ Keep customers updated about our compliance certifications and what we are working to support
- ☑ Make available the information you need to make decisions about our platforms
- ☑ Ensure our system has failover and redundancy built in
- ☑ Receive and manage vulnerability reports related to our products
- ☑ Adhere to the laws of the various jurisdictions we operate in

Your role

- □ Understand your risk profile and the sensitivity of your data
- □ Assess the suitability of our Cloud-based platforms based on the information we provide
- □ Ensure the platform is sufficient to meet your compliance needs
- □ Meet the agreed upon data breach disclosure and notification requirements when relevant
- □ Protect your endpoints through good security practices
- □ Only host permitted data on our platforms
- □ Operate within the law of the jurisdictions in which you operate

Users

What Atlassian does

- ☑ Develop and roll out security controls that empower you to manage your users effectively
- ☑ Monitor our platforms for bad or malicious use
- ☑ Provide domain verification and user claim capabilities for a centralized view of users across your cloud organization
- ☑ Provide the option for **Atlassian Access** for more efficiency and control by allowing you to connect your identity provider to (1) enforce SSO or 2FA/MFA and (2) automate SCIM user provisioning
- ☑ Provide implementation and user support via our team
- ☑ Develop products and features that encourage **organization-wide insights** on usage and growth

Your role

- ☐ Verify your domain if you want to centrally manage your accounts
- ☐ Approve user access to your data
- ☐ Periodically review the list of users with access to your data and remove access from anyone who shouldn't have it
- ☐ Determine **authentication policies in Atlassian Access** based on your users and organizational needs

If you have a verified domain:

- ☐ Implement strong user access management controls such as federated identity management (SAML), two-step verification, and password policies as needed based on your risk
- ☐ Monitor your organization's user accounts for harmful or malicious use
- ☐ Set a password policy appropriate for your business

If you don't have a verified domain, or if you grant access to users outside your domain:

- ☐ Communicate the importance of good password management to all users with access to your data
- ☐ Notify Atlassian of any unauthorized use of your account. Be aware of the risks of social login (see 'Credential re-use' below)

Information

What Atlassian does

- ☑ Access your data only if there is a specific support need to do so
- ☑ Notify you of any breach we become aware of that affects your data
- ☑ Maintain system-level back-ups (which includes your information)

Your role

- □ Set up your Atlassian products to reflect the information accessibility that fits your needs
- □ Create backups of your data

Marketplace Apps

What Atlassian does

- ☑ Ensure all Cloud apps meet a baseline of security. They are continuously scanned and reviewed for vulnerabilities when listed on the marketplace
- ☑ Verify the developers of Marketplace Apps
- ☑ Require the developed to publish their privacy policies Data privacy guidelines for developers
- ☑ Invite app vendors/partners can join our Cloud Security Participant or Cloud Fortified programs by investing in their own bug bounty program and increase support and reliability
- ☑ Maintain Forge, a program in which Atlassian hosts the Cloud apps and enables app vendors to more easily leverage our infrastructure investments to meet higher security and reliability standards

Your role

- □ Assess the suitability of any Marketplace Apps you want to use based on the information they provide
- □ Notify Atlassian of any malicious behavior identified in a Marketplace App

Threat management

Preparation is key

Our security team is a big proponent of threat modeling, and spends a lot of time considering the scenarios we need to look out for, and the 'plays' we will run if and when we see those scenarios eventuate. We thought it might help to share with you some of the threats that you may need to consider when using our applications. Hopefully, these will help bring to life the joint responsibility we've outlined above. For additional information, you can find our security practices at **Security practices**.

Credential guessing

A malicious user may be able to guess a correct username and password combination and gain access to your account. Having strong passwords, and enabling multi-factor authentication, are the best controls to manage those risks. As noted in our guiding principles, if we see something affecting lots of users, we'll do our best to shut it down.

Credential re-use

If one or more of the accounts you have permitted to access your data uses the same email address and password combination elsewhere on the Internet, a compromise of that site may expose your data to attackers. Similarly, approving access for users who use social login introduces a risk to your data in the event of a breach of that user's social account. Good security awareness across your user base (including third parties you have granted access), and two-step verification are strong controls.

Man-in-the-middle attacks

An attack that seeks to insert itself between your browser and our server relies on you accepting the malicious system's certificate as valid. We will set up our systems to make this as hard as we can for an attacker, but security awareness and certificate inspection are best practices.

Endpoint compromise

The compromise of one of your endpoints (whether your laptop, desktop, tablet, or smartphone) will render all other controls ineffective. The using of up-to-date security software and keeping your systems fully patched are the best controls.

Malicious Marketplace Apps

Once you install and grant permissions to a Marketplace app, we will not be able to prevent that app from taking the actions allowed under those permissions, even if you don't approve of those actions. Reviewing the suitability of the app and the reasonableness of the requested permissions prior to installation is recommended.

Phishing or fake sites

As a cloud-based system, anyone can set up a website purporting to be us. Making sure that you're at the right site is important to ensure your data stays safe. Typing the URL into the browser directly, or using a bookmarked link is a good mitigation, and checking the certificate is worthwhile if in doubt.

Shared responsibility and shared success

In summary...

When it comes to reliability, security, privacy and compliance of the Atlassian Cloud, we are on the same team, and we both have important roles to play. We bring our strong team of security professionals working day and night to ensure security is built in to our products, to monitor for potential risks and attacks, and to respond rapidly when they're identified. We need you to help by establishing the effectiveness of your user access management, being conscious of the information you enter, making sure your endpoints are well managed, and verifying all Marketplace apps are appropriate and trustworthy.

Want to dig deeper?

Trust @ Atlassian

Security Practices

Atlassian Cloud Security Whitepaper

Atlassian Cloud and Architectural Practices

Privacy @ Atlassian

Privacy Policy

Cloud Terms of Service

Atlassian Compliance Resource Center

Learn more at
atlassian.com/trust

ATLASSIAN